IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

BEFORE THE HONORABLE SPENCER WILLIAMS, JUDGE

ROGER SCHLAFLY, PLAINTIFF, VS. PUBLIC KEY PARTNERS AND RSA DATA SECURITY, INC., DEFENDANTS.	NO. C-94-20512 SW
RSA DATA SECURITY, INC., PLAINTIFF, VS. CYLINK CORPORATION AND CARO-KANN CORPORATION, ET AL., DEFENDANTS.	NO. C-96-20094 SW
	SAN JOSE, CA WEDNESDAY OCTOBER 2, 1996 VOLUME 2 PAGES 148-296 MARKMAN HEARING

ORIGINAL

239

APPEARANCES:

FOR THE PLAINTIFF ROGER SCHLAFLY:

DR. ROGER SCHLAFLY
P.O. BOX 1680
SOQUEL, CA 95073

APPEARANCES CONTINUED ON NEXT PAGE

COURT REPORTER: SARA LERSCHEN, CSR #6213, RMR, CRR
COURT REPORTER

COMPUTERIZED TRANSCRIPTION BY XSCRIBE

APPEARANCES: (CONTINUED)

FOR RSA DATA SECURITY, INC.:
HELLER, EHRMAN, WHITE & MC AULIFFE
525 UNIVERSITY AVENUE
PALO ALTO, CA 94301-1900
BY: ROBERT T. HASLAM
ROBERT D. FRAM
BETH MITCHELL
ROBERT B. HAWK
ATTORNEYS AT LAW

FOR CYLINK CORPORATION, CARO-KANN CORPORATION AND STANFORD UNIVERSITY:
MORRISON & FOERSTER, LLP
755 PAGE MILL ROAD
PALO ALTO, CA 94304-1018
BY: KARL J. KRAMER
JANA G. GOLD
ATTORNEYS AT LAW

MORRISON & FOERSTER LLP
345 CALIFORNIA STREET
SAN FRANCISCO, CA 94104
BY: RAOUL D. KENNEDY
ATTORNEY AT LAW

ALSTON & BIRD
ONE ATLANTIC CENTER
1201 W. PEACHTREE STREET
ATLANTA, GEORGIA 30306
BY: PATRICK J. FLINN
ATTORNEY AT LAW

I N D E X

WEDNESDAY-OCTOBER 2, 1996 9:48 A.M.

THE COURT: OKAY. WHAT'S UP?

MR. FRAM: GOOD MORNING, YOUR HONOR. WE HAVE ONLY A COUPLE OF HOUSEKEEPING ITEMS FOR OUR EVIDENTIARY PRESENTATION, OUR WITNESSES HAVING BEEN CALLED AND EXAMINED FOR RSA. AND I'D JUST LIKE TO MARK A FEW ADDITIONAL EXHIBITS.

THE FIRST EXHIBIT I'D LIKE TO MARK IS PLAINTIFF'S EXHIBIT 1005. IT IS AN EXCERPT FROM CYLINK AND CARO-KANN'S SUPPLEMENTAL RESPONSES TO RSA'S FIRST SET OF INTERROGATORIES. IT'S BEING MARKED WITH THE UNDERSTANDING THAT DEFENDANTS MAY WANT TO PROVIDE THE COMPLETE DOCUMENT. WE HAVE PROVIDED EXCERPTS, TRYING TO SAVE SOME PAPER IN THIS CASE.

WE'RE ALSO MARKING AT THIS TIME PLAINTIFF'S EXHIBITS 1006-A AND B. AND THESE ARE EXCERPTS OF DEPOSITION TESTIMONY OF LAWRENCE C. WASHINGTON.

1006-A SETS FORTH FOUNDATION TESTIMONY FROM MR. WASHINGTON, ESTABLISHING THAT HE IS, IN FACT, OUTSIDE THE JURISDICTION IN HIS ORDINARY PROFESSIONAL RESIDENCE, AND THAT HE WAS SPONSORED BY DEFENDANTS IN THE CASE OF CYLINK V. RSA.

AND 1006-B CONTAINS SUBSTANTIVE --

THE COURT: "B," AS IN "BOY"?

MR. FRAM: "B," AS IN "BOY," CONTAINS

SUBSTANTIVE TESTIMONY FROM MR. WASHINGTON REGARDING THE MEANING OF TERMS DISCUSSED YESTERDAY, SUCH AS "SECURE" AND "COMPUTATIONALLY SECURE."

FINALLY, YOUR HONOR, WE'D LIKE TO MARK AS EXHIBIT 1002, THAT WAS SKIPPED OVER AND OVER YESTERDAY, A DOCUMENT THAT WAS DISCUSSED IN THE TESTIMONY, WHICH IS A DRAFT, A 1977, MAY 7, 1977 DRAFT OF A DOCUMENT ENTITLED "HIDING INFORMATION AND RECEIPTS IN TRAP DOOR KNAPSACKS," BY RALPH MERKLE AND MARTIN HELLMAN.

(WHEREUPON, RSA'S EXHIBITS 1002, 1005, 1006-A AND 1006-B WERE MARKED FOR IDENTIFICATION.)

MR. FRAM: WE WERE GOING TO MOVE THESE INTO EVIDENCE, YOUR HONOR, ALONG WITH THE OTHER EXHIBITS MARKED AT THE CLOSE OF THE HEARING, AS PREVIOUSLY DISCUSSED WITH THE COURT AND AS PER AGREEMENT WITH OPPOSING COUNSEL, THE THOUGHT BEING AT THAT TIME, THE PARTIES WOULD NOT ARGUE EVIDENTIARY OBJECTIONS BUT WOULD RATHER SUBMIT A SHORT PAPER ON THEM TO THE COURT, SO AS TO BE ABLE TO STREAMLINE THIS HEARING.

THE COURT: ALL RIGHT. YES, SIR?

MR. KRAMER: KARL KRAMER ON BEHALF OF CYLINK AND CARO-KANN. I CONCUR THAT WE WILL ARGUE ABOUT THESE MATTERS WHEN WE ARE DONE WITH THE ARGUMENT TODAY. BUT I DID NOTE THAT --

THE COURT: ARGUE WITH YOURSELF OR ARGUE WITH ME?

MR. KRAMER: ARGUE AMONG OURSELVES.

THE COURT: OKAY.

MR. KRAMER: HOPEFULLY IN A WAY THAT IS HELPFUL FOR YOU.

BUT I DO KNOW THAT MR. FRAM'S CHARACTERIZATION OF THE TESTIMONY OF MR. WASHINGTON IS INCORRECT, AND I THINK IT WAS INAPPROPRIATE ARGUMENT NOW. AND WE'LL RAISE THAT LATER. OKAY?

THE COURT: OKAY. THANK YOU.

MR. FRAM: I'M SURE THEY WILL.

SO WITH THAT, YOUR HONOR, THAT CONCLUDES OUR EVIDENTIARY PRESENTATION. AND I THINK WE'RE READY FOR, I SUPPOSE, DEFENDANTS' WITNESSES OR PRESENTATION, IF ANY, OR THE OTHER PARTIES.

THE COURT: OKAY.

MR. KENNEDY: YOUR HONOR, ON BEHALF OF CYLINK AND CARO-KANN, WE HAVE NO LIVE TESTIMONY, YOUR HONOR.

THE COURT: ALL RIGHT.

MR. FLINN: STANFORD UNIVERSITY HAS NO LIVE TESTIMONY, YOUR HONOR.

THE COURT: OKAY. ANY DEAD TESTIMONY?

(LAUGHTER.)

THE COURT: GO AHEAD. ARE YOU GOING TO PRESENT

DEPOSITIONS?

MR. FLINN: YES, YOUR HONOR. I BELIEVE THAT ALL OF THE DEFENDANTS HAVE, WITH THEIR VARIOUS PAPERS, SUBMITTED DEPOSITION EXCERPTS AND TREATISES AND THE LIKE. THERE MAY BE A FEW MORE DOCUMENTS THAT WILL COME IN. BUT IN TERMS OF HAVING A WITNESS GET UP AND EXPRESS AN OPINION, THERE IS NO SUCH WITNESS.

THE COURT: FINE. ALL RIGHT. OKAY. NEXT?

MR. SCHLAFLY: I'D JUST LIKE TO SAY I DON'T KNOW WHO LAWRENCE WASHINGTON IS, SO I'D LIKE TO RESERVE MY RIGHT TO OBJECT TO THAT EVIDENCE.

THE COURT: ALL RIGHT.

MR. SCHLAFLY: AND I'D LIKE TO TESTIFY ON MY BEHALF IN THIS CASE NOW.

THE COURT: AT THIS TIME?

MR. SCHLAFLY: YES.

MR. KRAMER: YOUR HONOR, ON BEHALF OF CYLINK AND CARO-KANN, I DON'T WANT TO DELAY THE PROCEEDINGS AT ALL, BUT I WANT TO MAKE SURE THAT THE NORMAL OBJECTIONS WE WOULD MAKE TO QUESTIONS AND ANSWERS WOULD BE RESERVED FOR THE END, BECAUSE TYPICALLY, WE HAVE AN OPPORTUNITY TO OBJECT TO A QUESTION AND ANSWER BEFORE THE ANSWER COMES. I DON'T KNOW HOW IT'S GOING TO WORK.

THE COURT: IS THIS THE SITUATION WHERE THE WITNESS ASKS HIMSELF A QUESTION?

MR. KRAMER: I THINK WE COULD DISPENSE WITH THAT, AS LONG AS WE UNDERSTAND AT THE END WE MAY HAVE SOME OBJECTIONS TO THE TESTIMONY.

THE COURT: FINE.

WILL YOU SWEAR THE WITNESS, PLEASE?

ROGER SCHLAFLY

CALLED AS A WITNESS BY THE PLAINTIFF ROGER SCHLAFLY, FIRST BEING DULY SWORN, TESTIFIED AS FOLLOWS:

THE WITNESS: YES.

THE CLERK: PLEASE STATE YOUR FULL NAME FOR THE RECORD.

THE COURT: HOW LONG DO YOU EXPECT TO BE, MR. SCHLAFLY? IT'S JUST A QUESTION OF INFORMATION. YOU CAN TESTIFY THERE, IF YOU LIKE.

THE WITNESS: FIFTEEN MINUTES.

THE COURT: EITHER WAY.

THE CLERK: WHAT IS YOUR OCCUPATION, SIR?

THE COURT: OCCUPATION?

THE WITNESS: I'M A FREELANCE MATHEMATICIAN.

THE CLERK: THANK YOU.

THE COURT: OKAY. HOW LONG DO YOU THINK YOU'LL BE?

THE WITNESS: 10 TO 15 MINUTES.

THE COURT: OKAY.

DIRECT TESTIMONY

THE WITNESS: OKAY. I'D LIKE TO TESTIFY WITH REGARD TO TWO ISSUES, TWO TECHNICAL ISSUES OF DISPUTE IN THIS CASE.

ONE IS THE MEANING OF THE TERMS. I THINK THE MOST CRUCIAL TERM THAT NEEDS TO BE CONSTRUED IN THESE PATENT CLAIMS IS THE TERM "COMPUTATIONALLY INFEASIBLE." AND CLOSELY RELATED TO THAT IS THE TERM "SECURE."

THE COURT: OKAY. WE COVERED A DISCUSSION ON THAT, SO I'D LIKE TO HEAR WHAT YOU HAVE TO SAY ABOUT IT.

COMPUTATIONALLY INFEASIBLE; RIGHT?

THE WITNESS: CORRECT.

THE COURT: OKAY.

THE WITNESS: I THINK THE TERM "COMPUTATIONALLY INFEASIBLE" IS DEFINED IN THE PATENT, BUT THERE IS A CONFUSING ASPECT ABOUT THE DEFINITION THAT I WOULD LIKE TO ADDRESS.

THAT IS, IN THE PATENT --

THE COURT: CAN YOU TELL ME -- FROM WHAT I'VE HEARD, WHAT MY THINKING IS RIGHT NOW ON THE SUBJECT -- IT'S BEEN DISCUSSED, ALTHOUGH THIS IS NOT CONCLUSIVE -- BUT THAT THE INTERCEPTOR OF THE MESSAGE DOES NOT HAVE ENOUGH TIME TO COMPUTE AND DECODE THE MESSAGE DUE TO THE TIME THAT WOULD BE FEASIBLE TO DO SO.

IN OTHER WORDS, WE TALKED ABOUT HOW LONG IT TAKES NOW AND THEN PREVIOUSLY, OR IT MIGHT IN THE FUTURE.

SO THAT THE COMPUTATIONALLY SECURE DEPENDS ON THE PERIOD OF TIME IN WHICH IT'S COMPUTATIONALLY INFEASIBLE, WHEN IT CAN'T ACTUALLY USE ENOUGH TIME TO TRY ALL THE VARIOUS THINGS TO SEE WHAT THE REAL MESSAGE IS. THAT'S IN LAYMAN'S TERMS.

THE WITNESS: I THINK THAT'S A GOOD DEFINITION, YOUR HONOR, AND IT'S CONSISTENT WITH THE PATENT.

THE COURT: THANK YOU.

THE WITNESS: I WOULD JUST LIKE TO ADDRESS ONE THING THAT I THINK IS CONFUSING ABOUT THE DEFINITION IN THE PATENT. SO LET ME REFER TO EXHIBIT 13, THE HELLMAN-MERKLE PATENT, COLUMN FIVE.

IT SAYS: "A TASK IS CONSIDERED COMPUTATIONALLY INFEASIBLE IF ITS COST AS MEASURED BY EITHER THE AMOUNT OF MEMORY USED OR THE COMPUTING TIME IS FINITE BUT IMPOSSIBLY LARGE."

THE COURT: OKAY.

THE WITNESS: THAT'S A DEFINITION WHICH I THINK IS OKAY, AND COMPLETELY CONSISTENT WITH WHAT YOU SAID.

THEN IT SAYS: "FOR EXAMPLE, ON THE ORDER OF TEN TO 30 OPERATIONS WITH EXISTING COMPUTATIONAL METHODS AND EQUIPMENT."

NOW, IF THAT'S JUST AN EXAMPLE, MAYBE WE DON'T NEED TO TAKE IT TOO SERIOUSLY. BUT I THINK WE NEED TO ANALYZE EXACTLY WHAT IS MEANT BY THIS SENTENCE.

AND THE SENTENCE SAYS TWO THINGS -- WELL, IT SAYS ABOUT THREE THINGS. I MEAN, IT SAYS APPROXIMATELY TEN TO 30 OPERATIONS. WELL, I DON'T THINK WE HAVE ANY SERIOUS QUIBBLES ABOUT THAT. IT'S TEN TO THE 20 OPERATIONS, TEN TO THE 40 OPERATIONS. I DON'T THINK WE'RE GOING TO HAVE A BIG DISAGREEMENT THERE.

AND THEN IT REFERS TO EXISTING COMPUTATIONAL METHODS AND ALSO EXISTING COMPUTATIONAL EQUIPMENT. "COMPUTATIONAL EQUIPMENT" REFERS TO COMPUTERS. COMPUTERS TODAY ARE PRETTY MUCH THE SAME AS THEY WERE 20 YEARS AGO. THEY'VE GOTTEN FASTER AND CHEAPER, BUT I DON'T THINK WE HAVE ANY SERIOUS DISPUTES ABOUT THAT.

THE TRICKY THING TO INTERPRET IS THE PHRASE "EXISTING COMPUTATIONAL METHODS." AND I THINK THERE ARE TWO WAYS TO INTERPRET THAT.

ONE WAY TO INTERPRET THAT IS TO REFER TO THE LOW-LEVEL COMPUTER OPERATIONS THAT A COMPUTER DOES WHEN --

THE COURT: IT'S ALL MATHEMATICAL; RIGHT? EVERYTHING IS MATHEMATICAL?

THE WITNESS: IT'S ALL MATHEMATICAL, YES.

THE COURT: OKAY.

THE WITNESS: BUT THERE ARE LOW-LEVEL METHODS AND THERE ARE HIGH-LEVEL METHODS.

WHEN A COMPUTER DOES A CALCULATION AT THE LOWEST LEVEL, YOU COULD LOOK AT ITS METHODS AS BEING THINGS SUCH

AS STORING NUMBERS IN MEMORY, RANDOMLY ACCESSING CERTAIN PARTS OF MEMORY, LOADING NUMBERS INTO REGISTERS, ADDING NUMBERS IN THE REGISTERS, MULTIPLYING NUMBERS IN THE REGISTER, WRITING THOSE OUTPUT.

THE COURT: THEY'RE ALL EXISTING METHODS?

THE WITNESS: THOSE WOULD ALL BE CONSIDERED EXISTING COMPUTATIONAL METHODS.

HOWEVER, ONE COULD ALSO INTERPRET THAT PHRASE "EXISTING COMPUTATIONAL METHODS" IN TERMS OF HIGHER-LEVEL ALGORITHMS. FOR EXAMPLE, IF SOMEONE FINDS A NEW METHOD FOR, WELL, IN THIS CASE, IT'S GOING TO BE FOR BREAKING THE KNAPSACK. IF SOMEBODY FINDS SOME NEW METHOD, SOME CLEVER ALGORITHM FOR MAKING SOME CRYPTOSYSTEM, IS THAT TO BE INTERPRETED AS ONE OF THE EXISTING COMPUTATIONAL METHODS OR NOT?

SO, I THINK THIS SENTENCE, THIS PHRASE IN THE PATENT, "EXISTING COMPUTATIONAL METHODS" TO REFER TO THESE LOW-LEVEL METHODS OR THE HIGH-LEVEL METHODS, I DON'T ACTUALLY KNOW FOR A FACT WHICH IS INTENDED. I THINK IT'S A LITTLE BIT AMBIGUOUS. IT COULD BE INTERPRETED EITHER WAY.

HOWEVER, IT IS MY BELIEF, BASED ON THE CONTEXT OF THE INVENTION AND THE SUPPORTING SPECIFICATION AND DOCUMENTS, THAT WHAT WAS MEANT BY THAT IS THE EXISTING -- THE LOW-LEVEL METHODS, OR THE EXISTING COMPUTATIONAL

METHODS.

THE COURT: OKAY.

THE WITNESS: AND HERE IS MY REASON FOR THINKING SO.

THE INVENTORS WERE INSPIRED TO THIS INVENTION LARGELY BY COMPUTER COMPLEXITY THEORY. AND COMPUTER COMPLEXITY THEORY IS CONCERNED WITH WHAT TYPES OF COMPUTATIONS ARE POSSIBLE AND HOW MANY OPERATIONS ARE NECESSARY TO DO A PARTICULAR COMPUTATION.

NOW, LET ME GIVE YOU AN ANALOGY HERE THAT MIGHT MAKE THINGS A LITTLE SIMPLER. LET'S SUPPOSE YOU'RE TRYING TO FIGURE OUT HOW FAR IT IS TO DRIVE TO NEW YORK. NOW, IT'S ABOUT 3,000 MILES, IF YOU GO DIRECTLY. IF YOU GO A LONG ROUTE, IT MIGHT BE FOUR- OR 5,000 MILES. BUT SINCE THERE ARE A LOT OF DIFFERENT ROADS YOU COULD TAKE, YOU COULD CONSIDER THAT A PROBLEM IN COMPUTATIONAL COMPLEXITY THEORY.

AND SOMEONE IN COMPLEXITY THEORY MIGHT WANT TO SAY -- MIGHT WANT TO ASK THE QUESTION, "WHAT IS THE SHORTEST ROUTE TO NEW YORK?"

AND SOMEONE IN COMPLEXITY THEORY MIGHT REASONABLY SAY, "WELL, I DON'T KNOW EXACTLY THE SHORTEST ROUTE, BUT WE CAN GET THERE IN 3,000 MILES, BUT THERE IS NO WAY TO GET THERE IN 2,000 MILES. IT'S JUST IMPOSSIBLE."

AND WHEN HE SAYS THAT, ABOUT GETTING TO NEW YORK IN 2,000 MILES, HE MEANS IT'S IMPOSSIBLE. HE DOESN'T MEAN THAT, WELL, ACCORDING TO THE ROUTES THAT ARE POPULARLY LOOKED AT AND POPULARLY TRAVELED, IT MEANS THERE IS NO ROUTE LESS THAN. HE MEANS IT IS IMPOSSIBLE TO GET THERE IN LESS THAN 2,000 MILES.

AND THAT IS WHAT PEOPLE IN COMPUTER COMPLEXITY THEORY ARE CONCERNED WITH. WHEN THEY SAY SOME PROBLEM IS DIFFICULT, THEY USUALLY MEAN THAT -- THEY USUALLY MEAN THAT IT'S IMPOSSIBLE TO SOLVE THE PROBLEM IN SOME SHORT NUMBER OF STEPS. NOW, THEY CAN'T ALWAYS --

THE COURT: MILEAGE IS A CONSTANT; ISN'T IT? THERE IS NO FLEXIBILITY OF THE MILES YOU'RE TALKING ABOUT.

THE WITNESS: WELL, YOU CAN TAKE DIFFERENT ROADS.

THE COURT: WELL, THE MINIMUM, WORKING WITH THE QUICKEST TIME AND SHORTEST ROUTE, IT'S IMPOSSIBLE TO GO THERE IN LESS THAN 3,000 MILES, AS YOU SAID.

THE WITNESS: THAT'S RIGHT.

THE COURT: WHEN YOU'RE TALKING ABOUT TIME ELEMENT, IF YOU INCREASE THE SPEED, THE WAY THIS COMPUTER WORKED, THEN THAT'S POSSIBLE.

THE WITNESS: WELL, IF YOU MEASURE IT IN TERMS -- IF YOU MEASURE THE COMPLEXITY IN TERMS OF THE NUMBER OF OPERATIONS, THEN THE SPEED OF THE COMPUTER

DOESN'T MAKE ANY DIFFERENCE. IT WILL DO THOSE OPERATIONS FASTER, BUT IT WON'T MAKE ANY DIFFERENCE.

NOW, THERE IS AN INHERENT -- IF YOU INVENT SOME COMPUTER THAT'S ABLE TO DO MORE WORK IN ONE OPERATION, THEN THERE WILL BE SOME DIFFERENCE, AND YOU'LL HAVE TO MAKE SOME ASSUMPTIONS AS TO WHAT KIND OF COMPUTERS YOU'RE USING, AND WHAT KIND OF LOW-LEVEL COMPUTATIONAL METHODS YOU'RE USING.

BUT THE COMPUTER COMPLEXITY THEORISTS WILL WANT TO SAY THAT THERE IS -- THAT TO SAY THAT SOME PROBLEM IS HARD, THAT THERE IS NO METHOD -- THERE IS NO ALGORITHM FOR SOLVING THAT PROBLEM, JUST LIKE THERE IS NO WAY TO GET TO NEW YORK IN LESS THAN 2,000 MILES.

AND I THINK THE EVIDENCE THAT THE INVENTORS WERE INSPIRED BY COMPLEXITY THEORY IS IN THEIR PAPERS THAT THEY WROTE, PAPERS -- IN THE NEW DIRECTIONS PAPER, DIFFIE AND HELLMAN TALK ABOUT COMPLEXITY THEORY. AND BASED ON THAT, I INTERPRET THE PHRASE "EXISTING COMPUTATIONAL METHODS" TO MEAN THE LOW-LEVEL METHODS, NOT THE HIGH-LEVEL METHODS. OKAY?

THE COURT: OKAY.

THE WITNESS: OKAY. THERE IS ONE OTHER POINT I WANTED TO MAKE, AND THAT HAS TO DO WITH THE INTERPRETATION OF THE BROAD HELLMAN-MERKLE CLAIMS, SUCH AS CLAIM 6, WHICH IS OVER ON THE BOARD THERE, AND CLAIM 1.

A CENTRAL ISSUE IN THIS CASE IS, OF COURSE, WHETHER OR NOT THESE CLAIMS COVER THE WHOLE CONCEPT OF PUBLIC KEY CRYPTOGRAPHY. AND I -- MOST OF THESE ARGUMENTS ARE LEGAL ARGUMENTS, WHICH WE'LL MAKE LATER WHEN WE START ARGUING LEGAL THINGS.

BUT I JUST WANTED TO MAKE THE POINT THAT IF THE INVENTORS REALLY INTENDED TO COVER THE WHOLE CONCEPT OF PUBLIC KEY CRYPTOGRAPHY, THERE ARE A COUPLE OF THINGS THAT I THINK NEED TO BE EXPLAINED.

THE MAIN THING BEING THAT THE CONCEPT OF PUBLIC KEY CRYPTOGRAPHY IS EXPLAINED AND IS DISCLOSED IN THE DIFFIE-HELLMAN MULTIUSER PAPER, WHICH IS CITED AS PRIOR ART IN THE PATENT, AND BECAUSE THE INVENTORS WERE LATE FILING THEIR PATENT APPLICATION, IT IS PRIOR ART, AND THERE IS NO DISPUTE ABOUT THAT. IT IS PUBLISHED AND IS PRIOR ART, AND IT DOES DISCLOSE THE CONCEPT OF PUBLIC KEY CRYPTOGRAPHY, AND IT DOES IT VERY NICELY AND EXPLAINS THE WHOLE CONCEPT.

THE COURT: AND THE PART IN THE PATENT DISCLOSES LESS THAN THAT, OR CLAIMS LESS THAN THAT?

THE WITNESS: WELL, I'LL LET CYLINK EXPLAIN JUST WHAT THE DIFFERENCE IS. BUT THE MULTIUSER PAPER EXPLAINS THE CONCEPT OF PUBLIC KEY CRYPTOGRAPHY.

THE PATENT SPECIFICATIONS OF HELLMAN-MERKLE AND DIFFIE-HELLMAN -- HELLMAN-MERKLE IS WHAT WE'RE CONCERNED

WITH TODAY -- EXPLAINS THE TRAP DOOR KNAPSACK. THE TRAP DOOR KNAPSACK IS NOT DESCRIBED IN THE MULTIUSER PAPER.

SO THE MULTIUSER PAPER DESCRIBES THE CONCEPT OF PUBLIC KEY CRYPTOGRAPHY, COMPLETE WITH PUBLIC KEYS, PRIVATE KEYS, ONE-WAY FUNCTIONS, AND DIGITAL SIGNATURES; AND STANFORD LOOKED AT PAPERS SLIPPED INTO THE PUBLIC DOMAIN BEFORE FILING FOR THIS PATENT.

AND THEN THIS PATENT DISCLOSES THE TRAP DOOR KNAPSACK AND A COUPLE OF VARIATIONS OF THE TRAP DOOR KNAPSACK.

AND THEN THIS PATENT HAS VERY BROAD CLAIMS. AND THESE VERY BROAD CLAIMS SEEM TO CLAIM THE WHOLE FIELD OF PUBLIC KEY CRYPTOGRAPHY, IF YOU READ THEM LITERALLY. AND I'M ARGUING HERE TODAY THAT I THINK IT'S QUESTIONABLE --

THE COURT: YOU'RE TESTIFYING.

THE WITNESS: I'M TESTIFYING; YES, I'M TESTIFYING.

THE COURT: OKAY.

THE WITNESS: I'M TESTIFYING AT THE MOMENT, AND I'LL BE ARGUING A SIMILAR POINT LATER ON.

MR. FLINN: ACTUALLY, YOUR HONOR, WHERE HE SAID MULTIUSER PAPER DESCRIBES THE BROAD CONCEPT OF PUBLIC KEY, THAT'S LEGITIMATE TESTIMONY.

BUT TO ARGUE FROM THE WITNESS STAND WHAT THE LEGAL CONSEQUENCES OF THAT ARE IS REALLY GOING BEYOND

TESTIMONY. HE'S FREE TO MAKE THAT, JUST FROM A DIFFERENT SPOT IN THE COURTROOM.

THE WITNESS: THANK YOU. THANK YOU.

THE COURT: OKAY.

THE WITNESS: HE'S QUITE CORRECT, AND I'LL TRY TO AVOID THAT.

THE ONLY POINT I WANT TO MAKE IS THAT THE MULTIUSER PAPER DOES DESCRIBE THE BROAD CONCEPT. IT'S VERY NICELY DESCRIBED. IT'S MY PROFESSIONAL OPINION THAT SOMEONE READING THE MULTIUSER PAPER CAN UNDERSTAND THE BROAD CONCEPT OF PUBLIC KEY ENCRYPTION AND ONE-WAY FUNCTIONS AND DIGITAL SIGNATURES AND ALL THAT STUFF.

AND I REGARD THAT AS EVIDENCE THAT THE INVENTORS IN THE HELLMAN-MERKLE PATENT WERE NOT INTENDING TO BE CLAIMING THE ENTIRE SUBJECT OF PUBLIC KEY CRYPTOGRAPHY, BECAUSE IT WAS ALREADY DISCLOSED IN ANOTHER PAPER THAT SLIPPED INTO THE PUBLIC DOMAIN. AND FURTHERMORE, THE LISTED INVENTORS ON THE HELLMAN-MERKLE PATENT ARE JUST HELLMAN AND MERKLE, WHEREAS, DIFFIE WAS A CO-AUTHOR OF THE MULTIUSER PAPER, AND EVIDENTLY, A CO-INVENTOR OF THE CONCEPT OF PUBLIC KEY CRYPTOGRAPHY.

AND IF, INDEED, THE HELLMAN-MERKLE PATENT WERE INTENDING TO COVER THE WHOLE CONCEPT OF PUBLIC KEY CRYPTOGRAPHY, THEN I DON'T UNDERSTAND WHY DIFFIE WAS NOT LISTED AS AN INVENTOR ON THE HELLMAN-MERKLE PATENT.

THAT'S ALL I HAVE TO SAY --

THE COURT: THANK YOU.

THE WITNESS: -- RIGHT NOW.

THE COURT: OKAY.

MR. FRAM: RSA HAS NO QUESTIONS FOR THIS WITNESS AT THIS TIME BUT RESERVES THE RIGHT, IF THERE IS ANYTHING FURTHER, IN LIGHT OF MR. FLINN'S QUESTIONS.

THE COURT: FINE. THANK YOU.

MR. FLINN: I'VE GOT A FEW, YOUR HONOR. IF I COULD HAVE A MINUTE?

THE COURT: YES, PLEASE, MR. FLINN.

CROSS-EXAMINATION

BY MR. FLINN: Q. MR. SCHLAFLY, YOU WERE PLEASANT ENOUGH TO JUMP RIGHT TO THE MEAT OF YOUR TESTIMONY VERY QUICKLY, BUT YOU OMITTED A FORMALITY THAT I ACTUALLY THINK WOULD BE VERY HELPFUL FOR US, WHICH IS TRADITIONAL, THAT AN EXPERT WITNESS LISTS HIS OR HER CREDENTIALS. AND I THINK YOU HAVE SOME SUBSTANTIAL ONES THAT WOULD BE HELPFUL FOR US.

COULD YOU TELL US A LITTLE BIT MORE ABOUT YOUR EDUCATION, YOUR EXPERIENCE IN WRITING COMPUTER PROGRAMS THAT DO CRYPTOGRAPHY, YOUR EXPERIENCE IN WRITING COMPUTER PROGRAMS THAT DO PUBLIC KEY CRYPTOGRAPHY?

A. SURE. I RECEIVED A PH.D. IN MATHEMATICS FROM THE UNIVERSITY OF CALIFORNIA AT BERKELEY IN 1980.

I'VE WORKED IN CRYPTOGRAPHY ON AND OFF FOR TEN OR 15 YEARS, AND IN THAT PROCESS, I'VE DEVELOPED SOME COMPUTER SOFTWARE, WHICH IMPLEMENTS CRYPTOGRAPHY AND PUBLIC KEY CRYPTOGRAPHY, SOME OF WHICH HAS BEEN SOLD ON MICROCOMPUTERS.

Q. YOU'VE HEARD OF A COMPUTER PROGRAM KNOWN AS PKZIP; IS THAT RIGHT?

A. YES.

THE COURT: PKZIP?

MR. FLINN: Q. COULD YOU DESCRIBE FOR US VERY BRIEFLY WHAT PKZIP IS?

A. PKZIP IS A FILE COMPRESSION PROGRAM FOR MOSTLY PERSONAL COMPUTERS. IT TAKES A COLLECTION OF FILES AND IT COMPRESSES THEM INTO A SMALLER SPACE AND PUTS THEM NEATLY TOGETHER IN ONE FILE WHERE THEY CAN BE CONVENIENTLY MOVED AROUND OR STORED OR BACKED UP.

Q. WOULD YOU AGREE WITH ME THAT THIS IS THE SINGLE MOST COMMON DATA COMPRESSION FILE COMPRESSION SOFTWARE IN USE IN PERSONAL COMPUTERS TODAY?

A. YES.

Q. AND IT'S DISTRIBUTED AS SHAREWARE, OR FORMS OF IT ARE DISTRIBUTED AS SHAREWARE?

A. YES.

Q. AND WHAT IS THAT, SHAREWARE?

A. SHAREWARE IS A MEANS OF DISTRIBUTING SOFTWARE. AND IT

WORKS BY DISTRIBUTING FREE SAMPLE VERSIONS, OR FULLY FUNCTIONAL, WORKING VERSIONS IN A FREELY AVAILABLE MANNER. AND THEN THE USER IS EXPECTED TO PAY FOR IT OR LICENSE IT IN SOME OTHER WAY IF HE DECIDES HE LIKES IT, AFTER SOME TRIAL USE.

Q. AND THE USER IS ON AN HONOR SYSTEM, TO SEND THE MONEY INTO THE DEVELOPER OF THE SHAREWARE, IN MOST CASES?

A. WELL, THAT'S THE WAY IT WORKS OUT. TECHNICALLY -- I MEAN, IN PRACTICE, THAT'S THE WAY IT WORKS OUT. TECHNICALLY, THE AUTHOR DOES HAVE A COPYRIGHT AND IS LEGALLY IN A POSITION TO ENFORCE THE COPYRIGHT.

Q. THAT'S FINE.

NOW, THE REASON I BRING THIS UP IS THAT PKZIP HAS A ENCRYPTION UTILITY IN IT OR FEATURE IN IT; DOESN'T IT, THE MORE RECENT VERSIONS OF IT?

A. YES, IT DOES.

Q. AND YOU WERE INVOLVED IN THE DEVELOPMENT OF THAT UTILITY; ISN'T THAT RIGHT?

A. YES, I WAS.

Q. AND WOULD YOU AGREE WITH ME THAT THAT ENCRYPTION UTILITY IS SOMETHING THAT IS USED WITH SOME FREQUENCY BY USERS OF PKZIP?

A. YES, I WOULD.

Q. SINCE YOU INSERTED PKZIP -- IT'S STILL TODAY, PEOPLE STILL USE THE ENCRYPTION UTILITY; DON'T THEY?

A. YES, THEY DO.

Q. BUT SINCE YOU DEVELOPED IT, PEOPLE, AS DR. KONHEIM SAID, IN THE CRYPTO COMMUNITY, LOOKED FOR WEAKNESSES IN YOUR UTILITY?

A. YES, THEY DID.

Q. AND SOME WERE FOUND?

A. YES.

Q. BUT PEOPLE STILL USE IT, EVEN THOUGH THERE WERE SOME WEAKNESSES FOUND IN IT?

A. PEOPLE USE PKZIP PRIMARILY FOR ITS COMPRESSION FEATURES, NOT ITS ENCRYPTION FEATURES.

Q. BUT PEOPLE STILL USE PKZIP ENCRYPTION; DON'T THEY, NOTWITHSTANDING THE FACT THAT WEAKNESSES HAVE BEEN FOUND?

A. THAT'S CORRECT.

Q. AND FOR A LOT OF USES, YOU'D AGREE WITH ME THAT THE PKZIP ENCRYPTION UTILITY THAT YOU DEVELOPED IS USEFUL?

A. YES.

Q. NOW, YOU HAVE ADDRESSED THE DEFINITION OF "COMPUTATIONALLY INFEASIBLE" IN YOUR EXPERT TESTIMONY. BUT I WANTED TO ASK YOU A LITTLE BIT ABOUT SOME OF THE OTHER TERMS IN THE CLAIMS.

YOU WERE HERE YESTERDAY DURING DR. KONHEIM'S TESTIMONY; IS THAT RIGHT?

A. YES, I WAS.

Q. AND YOU RECALL WHERE -- OTHER THAN THE TERMS "SECURE"

AND "COMPUTATIONALLY INFEASIBLE," YOU RECALL HIS TESTIMONY ABOUT NOT BEING ABLE TO UNDERSTAND THE MEANING OF ALL THE OTHER TERMS? DO YOU RECALL THAT TESTIMONY?

A. YES.

Q. DO YOU AGREE WITH HIM?

A. YOU'RE ASKING ME WHETHER OR NOT HE UNDERSTOOD THE TERMS?

Q. NO, NO.

DO YOU AGREE WITH HIM THAT ONE OF ORDINARY SKILL IN THE ART WOULDN'T KNOW WHAT ANY OF THOSE OTHER WORDS MEAN?

MR. HASLAM: OBJECTION. THAT MISCHARACTERIZES THE WITNESS' TESTIMONY.

THE COURT: PARDON ME?

MR. HASLAM: THAT MISCHARACTERIZES PROFESSOR KONHEIM'S TESTIMONY. IT WAS THAT THEY HAD NO WELL-UNDERSTOOD MEANING IN THE ART AND THAT HE NEEDED TO GO TO THE SPECIFICATION TO DETERMINE HOW TO ACCOMPLISH THAT. HE DIDN'T SAY HE DID NOT UNDERSTAND ANY OF THE PARTICULAR WORDS IN THE CLAIM. AS A MATTER OF FACT, I BELIEVE HE WAS ASKED THAT QUESTION YESTERDAY.

THE COURT: ALSO, I THINK YOU SHOULD SPECIFY THOSE TERMS INDIVIDUALLY.

MR. FLINN: WELL, IT MAY BE -- I'M TRYING TO SIMPLIFY THIS.

Q. BUT YOU RECALL DR. KONHEIM'S TESTIMONY ABOUT THE LACK OF A WELL-UNDERSTOOD MEANING ABOUT TERMS SUCH AS "PROCESS," "COMMUNICATE," "GENERATE," "TRANSFORM," "ENCIPHER," ET CETERA? DO YOU RECALL THAT TESTIMONY?

A. YES.

Q. DO YOU AGREE WITH THAT TESTIMONY, THAT THERE IS NO WELL-UNDERSTOOD MEANING OF THOSE TERMS IN THE ART?

A. WELL, HE HAD HIS OWN QUALIFICATIONS, THAT HE'S BETTER ABLE TO MAKE THAN I AM. I'D RATHER YOU JUST ASK ME -- IF YOU'RE ASKING ME SIMPLY WHETHER OR NOT THOSE TERMS HAVE A WELL-UNDERSTOOD MEANING IN THE ART, I WOULD SAY YES.

Q. DID YOU EVER GET A COPY OF DR. KONHEIM'S SLIDES THAT HE GAVE FROM HIS TUTORIAL?

A. YES, I RECEIVED A COPY AT THE BEGINNING OF HIS PRESENTATION.

Q. DO YOU HAVE A COPY WITH YOU NOW?

A. I BELIEVE IT'S ON MY TABLE OVER THERE JUST NEXT TO THE LAPTOP.

Q. DO YOU MIND IF MR. KRAMER GETS THAT FOR YOU?

A. NO, NOT AT ALL.

YES, I BELIEVE THAT'S IT.

Q. AND I WAS WONDERING IF THE COURT HAD ITS COPY.

THE COURT: I DO. I DO.

YES, I DO. OKAY. I HAVE IT. OKAY.

MR. FLINN: Q. DO YOU RECALL, GENERALLY, THE

ORDER OF DR. KONHEIM'S PRESENTATION?

A. YES.

Q. MORE SPECIFICALLY, HE TALKED ABOUT ENCRYPTION GENERALLY, AND THEN HE GOT INTO PUBLIC KEY CRYPTOGRAPHY, AND THEN HE BEGAN TO TALK ABOUT KNAPSACKS AND THE RSA METHOD AFTER THAT. DO YOU RECALL THAT?

A. YES. AND I'M LOOKING AT HIS OUTLINE IN FRONT OF ME.

Q. OKAY. AND IF YOU LOOK, THE DISCUSSION OF PUBLIC KEY BEGINS AT TAB THREE, AND THE DESCRIPTION OF KNAPSACK IS TAB FOUR, AND THEN RSA IS TAB SIX?

A. YES.

Q. AND YOU RECALL THAT HE DISCUSSED PUBLIC KEY GENERALLY IN HIS DISCUSSION OF TAB THREE AND THE SLIDES THERE WITHOUT DISCUSSING ANY PARTICULAR IMPLEMENTATION. DO YOU RECALL THAT?

A. YES.

Q. AND YOU RECALL IN HIS DISCUSSION, HE USED TERMS LIKE "PUBLIC KEY," "PRIVATE KEY," "MESSAGE," "ENCRYPT," "DECRYPT," IN HIS GENERAL DISCUSSION ABOUT PUBLIC KEY CRYPTOGRAPHY?

A. YES.

Q. AND WHEN HE USED THOSE WORDS IN HIS GENERAL DESCRIPTION ABOUT PUBLIC KEY CRYPTOGRAPHY, DID YOU UNDERSTAND WHAT HE MEANT?

A. I SHOULD SAY THAT WHILE HE WAS GIVING HIS

PRESENTATION, I WAS BUSY PREPARING MY SLIDES FOR MY SUBSEQUENT PRESENTATION. AND I DIDN'T PAY ATTENTION TO EVERY WORD HE SAID.

BUT I THINK I CAN ANSWER, YES, THAT WHAT I PAID ATTENTION TO, I UNDERSTOOD.

Q. YOU MENTIONED -- AND WE'RE GOING TO TALK NOW ABOUT YOUR DEFINITION OF -- OR THE DEFINITION YOU BELIEVE IS THE APPROPRIATE ONE FOR "COMPUTATIONALLY INFEASIBLE," BUT LET ME ASK A FUNDAMENTAL QUESTION OR A FOUNDATION QUESTION. YOU MENTIONED SOMETHING CALLED COMPLEXITY THEORY?

A. YES.

Q. DO YOU KNOW SOMEONE NAMED DONALD KNUTH, KNOW OF SOMEONE NAMED DONALD KNUTH?

A. I'VE NEVER MET HIM. I KNOW OF HIM.

Q. IS HE INVOLVED IN COMPLEXITY THEORY, AS IT INVOLVES COMPUTERS?

A. YES.

Q. IN WHAT WAY IS HE INVOLVED?

A. WELL, HE'S A STANFORD PROFESSOR, OR AN EMERITUS PROFESSOR. HE WROTE THAT BOOK THAT'S RIGHT IN FRONT OF YOU. AND HE WROTE -- HE'S WRITTEN A -- MANY PAPERS IN COMPUTER SCIENCE. AND I WOULD CONSIDER HIM AN AUTHORITY IN COMPUTER SCIENCE.

Q. WOULD YOU CONSIDER HIM AN AUTHORITY IN COMPLEXITY THEORY, AS IT APPLIES TO COMPUTER SCIENCE?

A. YES.

Q. WOULD YOU CONSIDER HIM A PRE-EMINENT AUTHORITY IN THAT AREA?

A. I WOULD CERTAINLY CONSIDER HIM AN AUTHORITY.

Q. NOT A PRE-EMINENT ONE?

A. WELL, WHAT DO YOU MEAN BY "PRE-EMINENT"?

THE COURT: HOW MANY LEVELS ABOVE HIM ARE THERE?

MR. FLINN: Q. AMONG THE TOP TEN IN HIS FIELD IN THE LAST 20 YEARS.

A. I'M NOT SURE I WOULD SAY THAT.

HE SPENT MUCH OF HIS TIME IN THE LAST 20 YEARS DEVOTED TO THE DEVELOPMENT OF PRACTICAL SYSTEMS THAT ARE PROBABLY NOT OF GREAT THEORETICAL IMPORTANCE IN COMPLEXITY THEORY.

Q. AS OF 1977, WOULD YOU PUT HIM IN THAT CLASS?

A. IN THE CLASS OF TOP TEN?

AGAIN, I DON'T KNOW. HE'S CERTAINLY A VERY AUTHORITATIVE PERSON AND DONE A LOT OF VERY IMPORTANT WORK. I MEAN, THE MOST EXCITING WORK IN THE '70S IN COMPLEXITY THEORY WAS DONE IN CONNECTION WITH THE N-P PROBLEM, WHERE THE BIGGEST CONTRIBUTIONS WERE DONE BY OTHERS.

I'M NOT PREPARED TO SAY THAT HE WOULD BE IN THE TOP TEN.

Q. THAT'S FINE.

A. AGAIN, ALSO, I MEAN, IT DEPENDS ON HOW YOU RANK PEOPLE. I MEAN, ARE YOU RANKING PEOPLE BASED ON THE SIGNIFICANCE OF THEIR RESEARCH CONTRIBUTIONS, OR ARE YOU RANKING PEOPLE BASED ON, YOU KNOW, THE OVERALL QUALITY OF THEIR SCHOLARLY WORK? ARE YOU RANKING -- I JUST CAN'T ANSWER THAT QUESTION.

Q. THAT'S FINE. I'M NOT GOING TO PRESS THE ISSUE ANY LONGER, DR. SCHLAFLY.

I WANT TO NOW TRY TO UNDERSTAND A LITTLE BIT ABOUT YOUR DEFINITION OF "COMPUTATIONALLY INFEASIBLE" AND SEE IF I CANNOT BE -- HAVING NEVER TAKEN A COURSE IN COMPLEXITY THEORY OR ANYTHING LIKE THAT, I JUST WANT TO TRY TO UNDERSTAND IT.

AND WHAT I'D LIKE TO DO, IF I COULD, IS PUT UP THAT EXCERPT FROM THE PATENT THAT YOU READ FROM, THAT DEFINITION OF "COMPUTATIONALLY INFEASIBLE," IF I COULD HAVE JUST A MOMENT TO DO THAT. I THINK IT'S HERE.

AND WHAT I WOULD LIKE TO DO IS PUT IT UP OVER HERE SO THERE IS MORE OF A CHANCE ALL OF US IN THE COURTROOM CAN SEE IT. BUT DR. SCHLAFLY, IF YOU CAN'T SEE IT, WE HAVE THE SAME DOCUMENT HERE.

WE'RE NOT GOING TO HAVE ONE FOR THE COURT, THAT IS, THE SAME DOCUMENT.

CAN YOU READ THAT FROM THERE WHERE YOU SIT, DR. SCHLAFLY?

A. YES, YES. I HAVE IT IN THE PATENT IN FRONT OF ME ANYWAY.

Q. AND WHAT I WANT TO FOCUS --

A. BUT BEFORE YOU ASK, YOU KEEP REFERRING TO MY DEFINITION. I BELIEVE I'M JUST INTERPRETING -- TRYING TO INTERPRET THE DEFINITION WHICH IS IN THE PATENT.

Q. I UNDERSTAND THAT. AND WHEN I REFER TO YOUR DEFINITION, WHAT I MEAN IS THE DEFINITION THAT IS YOUR OPINION AS THE CORRECT DEFINITION.

A. YES.

Q. THAT'S ALL.

AND YOU HAVE FOCUSED ON THE LAST CLAUSE, "EXISTING COMPUTATIONAL METHODS AND EQUIPMENT"; IS THAT RIGHT?

A. I JUST TESTIFIED ABOUT THAT PHRASE, YES.

Q. OKAY. NOW, "EQUIPMENT" YOU HAVE REFERRED TO AS HARDWARE; RIGHT?

A. YES.

Q. AND SO, IF I UNDERSTAND, JUST LOOKING AT THAT DEFINITION CORRECTLY, SOMETHING MIGHT MEET THE DEFINITION OF "COMPUTATIONALLY INFEASIBLE" IF, GIVEN EXISTING HARDWARE, IT WOULD BE IMPOSSIBLY LONG TO COMPUTE IT; RIGHT?

A. YES.

Q. OKAY. AND THE INVENTORS WERE AWARE THAT COMPUTERS

MIGHT GET VERY, VERY FAST IN THE FUTURE; RIGHT?

A. I'M SURE THE INVENTORS WERE AWARE OF THAT.

Q. AND YOU UNDERSTAND THAT'S WHY THEY LIMITED THE DEFINITION TO "EXISTING COMPUTATIONAL EQUIPMENT"; IS THAT RIGHT?

A. WELL, YOU'RE ASKING ME ABOUT THE INVENTOR'S INTENT. HE'S SITTING RIGHT OVER THERE. YOU COULD ASK HIM.

Q. WELL, YOU'VE OPINED, SIR, AS TO THE INVENTOR'S INTENT, AND I'M TRYING TO EXPLORE THAT A LITTLE BIT.

YOU'D AGREE WITH ME THAT THE INVENTORS, IN LIMITING IT, AT LEAST WITH RESPECT TO EXISTING COMPUTATIONAL EQUIPMENT, IS: THEY RECOGNIZED THE POSSIBILITY THAT FASTER COMPUTERS MIGHT BE INVENTED IN THE FUTURE, AND THEY WEREN'T GOING TO MAKE ANY REPRESENTATION THAT ANY SYSTEM WOULD BE INFEASIBLE FOR ALL COMPUTERS, NO MATTER WHAT ADVANCES IN SPEED MAY HAPPEN IN THE FUTURE; ISN'T THAT FAIR?

A. YES. AND THEY PRESUMABLY WANTED TO ADD SOME SPECIFICITY TO THEIR EXAMPLE.

Q. OKAY. AND ON COMPUTATIONAL METHODS, YOU SAID THAT THERE WERE TWO ALTERNATIVES. ONE MEANT EXISTING ALGORITHMS, AND THE OTHER, EXISTING LOW-LEVEL COMPUTER OPERATIONS, HOW THE ONES AND ZEROS ARE PASSED BACK AND FORTH INSIDE THE HARDWARE; IS THAT RIGHT?

A. AND THE WAY THE MEMORY AND THE REGISTERS AND THE

PROCESSOR WORKS, YES.

Q. WOULD IT BE FAIR TO SAY, TO SORT OF RESTATE THE DEFINITION YOU ARE PROPOSING, AS HAVING THREE ELEMENTS: TO BE COMPUTATIONALLY INFEASIBLE, IT'S GOT TO BE IMPOSSIBLY LARGE USING EXISTING EQUIPMENT, USING EXISTING ALGORITHMS, OR USING AS YET UNDEVELOPED ALGORITHMS. IS THAT ANOTHER FAIR WAY OF RESTATING YOUR DEFINITION?

A. AS THOSE BEING -- I'M NOT SURE WHAT YOU MEAN. DO YOU MEAN THREE ALTERNATIVES TO BE THERE?

Q. NO, NO. THERE ARE THREE REQUIREMENTS FOR THE DEFINITION OF COMPUTATIONALLY INFEASIBLE THAT YOU ARE PROPOSING. THE SYSTEM MUST BE COMPUTATIONALLY INFEASIBLE USING EXISTING COMPUTERS, AS OF 1977; IT MUST BE COMPUTATIONALLY INFEASIBLE USING EXISTING COMPUTERS USING KNOWN ALGORITHMS IN 1977; BUT IT ALSO MUST BE COMPUTATIONALLY INFEASIBLE USING EXISTING COMPUTERS RUNNING AS YET UNKNOWN ALGORITHMS?

A. OH, YEAH, YEAH.

Q. AND THE ALTERNATIVE DEFINITION, IF THE WORD "EXISTING COMPUTATIONAL METHODS" MEANS EXISTING ALGORITHMS, THEN THERE WERE ONLY TWO ELEMENTS THAT A SYSTEM MUST MEET IN ORDER TO FULFILL THE DEFINITION OF "COMPUTATIONALLY INFEASIBLE." THE SYSTEM MUST SIMPLY BE INFEASIBLE USING 1977-ERA EQUIPMENT AND 1977-ERA ALGORITHMS; IS THAT RIGHT?

A. WELL, I'M NOT SURE, BECAUSE, FOR ONE THING, THAT

LATTER PHRASE, ABOUT EXISTING COMPUTATIONAL METHODS AND EQUIPMENT, OCCURS IN AN EXAMPLE AFTER THE DEFINITION. AND HOW THAT LIMITS THE DEFINITION IS A MATTER OF SOME DEBATE.

SO THAT EVEN IF I AGREED -- EVEN IF I AGREED WITH YOU -- WELL, EVEN STATING THE POSITION, I GUESS -- EVEN IF WE CAME TO AN OPINION AS TO WHAT IS MEANT BY "COMPUTATIONAL METHODS," WE WOULD STILL HAVE TO DISCUSS HOW THAT EXAMPLE LIMITS THE DEFINITION.

Q. ALL RIGHT. LET ME ASK YOU TO ASSUME IT IS A HYPOTHETICAL QUESTION, BECAUSE WHAT MY REAL PURPOSE IS IS TO ILLUSTRATE THE DIFFERENCES BETWEEN THE DEFINITION YOU ARE PROFFERING AND AN ALTERNATIVE DEFINITION.

LET ME ASK YOU TO ASSUME, FOR PURPOSES OF ARGUMENT ONLY, A DEFINITION OF "COMPUTATIONALLY INFEASIBLE" WHICH ONLY HAS TO MEET THOSE TWO REQUIREMENTS: 1977-ERA EQUIPMENT, AND 1977-ERA ALGORITHMS.

DOES THAT MAKE SENSE TO YOU, SIR? IS THAT SOMETHING YOU CAN UNDERSTAND AS AN ASSUMPTION FOR FURTHER QUESTIONS?

A. IT'S VERY DIFFICULT TO SAY WHAT A 1977-ERA ALGORITHM IS.

ALGORITHMS GET DEVELOPED, AND USING -- I MEAN, IT'S EASY TO SAY WHAT A 1977 COMPUTER IS BECAUSE YOU CAN GO PULL IT OFF THE SHELF IN A STORE. WHAT A 1977 ALGORITHM IS IS MUCH HARDER, BECAUSE IT'S JUST NOT SO

EASILY DEFINED.

Q. I UNDERSTAND THAT. BUT LET'S USE THE EXAMPLE THAT YOU PROFFERED IN YOUR TESTIMONY, THE TRAP DOOR KNAPSACK.

YOU'D AGREE WITH ME THAT THE ALGORITHM FOR BREAKING THE SIMPLEST OF THE KNAPSACKS TAUGHT IN THE PATENT WAS NOT PUBLISHED UNTIL 1982?

A. YES, THAT'S CORRECT. I MEAN, IT'S HARD TO SAY EXACTLY HOW MUCH OF THAT ALGORITHM WAS BRAND NEW AND HOW MUCH OF IT USED PREVIOUS TECHNIQUES.

Q. LET'S, JUST SO THAT WE CAN ILLUSTRATE THE DIFFERENCE, ASSUME THAT A KNOWN ALGORITHM IS ONE THAT ACTUALLY EFFECTIVELY BREAKS THE SYSTEM OR SOME EMBODIMENT OF IT AND IS PUBLISHED, SO THAT PEOPLE KNOW ABOUT IT. CAN WE NOW WORK WITH THAT ALTERNATIVE DEFINITION FOR SOME FURTHER QUESTIONS?

A. TO BE A KNOWN ALGORITHM TO BE PUBLISHED?

Q. YES.

A. WELL, I MEAN, I GUESS I CAN USE THAT AS A WORKING DEFINITION FOR SOME PURPOSES.

HOWEVER, I THINK THERE ARE A LOT OF AMBIGUITIES THERE. I MEAN, LIKE, FOR EXAMPLE, IF YOU ASKED ME WHEN WAS THE FAST FOURIER TRANSFORM PUBLISHED, I WOULD SAY, WELL, THE FIRST PAPER THAT EXPLICITLY SET THAT OUT IN DETAIL WOULD HAVE BEEN ABOUT 1965.

ON THE OTHER HAND, THERE ARE PAPERS, YOU KNOW,

50 YEARS EARLIER THAT HAVE ALMOST THE EXACT SAME FORMULAS THAT, YOU KNOW, THAT -- AND HAVE ALMOST THE EXACT SAME IDEAS. THEY JUST DIDN'T LAY IT OUT IN THAT MANNER AND CALL IT THAT.

Q. I PROMISE YOU, SIR, THAT I WON'T EVEN ASK YOU ABOUT THAT, BECAUSE I DON'T THINK I CAN PRONOUNCE IT. I'VE GOT SOME OTHER QUESTIONS FOR YOU.

YOU WOULD AGREE WITH ME, WOULD YOU NOT, THAT THE INVENTORS DID NOT CLAIM THAT THE TRAP DOOR KNAPSACK WAS INVULNERABLE TO UNKNOWN ALGORITHMS IN 1977?

A. NO, I DON'T THINK I WOULD.

Q. AND WHY NOT?

A. I THINK THE INVENTORS BELIEVED THAT THE KNAPSACK PROBLEM WAS SOMETHING THAT IS COMPUTATIONALLY DIFFICULT, IN THE SENSE THAT THERE ARE NO ALGORITHMS FOR BREAKING IT, KNOWN OR UNKNOWN.

Q. WHERE DID THEY SAY THERE ARE NO ALGORITHMS FOR BREAKING IT, KNOWN OR UNKNOWN?

A. WELL, THOSE ARE MY WORDS. BUT LET ME -- LET ME LOOK AT THE DOCUMENTS FOR A MOMENT.

OKAY. IF YOU TURN TO EXHIBIT 13 --

Q. ARE YOU REFERRING TO THE PATENT?

A. YES, THE HELLMAN-MERKLE PATENT.

Q. YES.

A. AND COLUMN TWO, THE SENTENCE STARTING AT LINE 43, IT

SAYS:

"THE ILLUSTRATED EMBODIMENT DIFFERS FROM PRIOR APPROACHES TO A PUBLIC KEY CRYPTOSYSTEM, AS DESCRIBED IN MULTIUSER CRYPTOGRAPHIC TECHNIQUES, IN THAT IT'S BOTH PRACTICAL TO IMPLEMENT AND IS DEMONSTRABLY INFEASIBLE TO EMBARK USING KNOWN METHODS."

Q. NOW, IF "KNOWN METHODS" MEANS ALGORITHMS, AREN'T THEY SAYING THAT IT'S INFEASIBLE ONLY WITH RESPECT TO KNOWN ALGORITHMS, AND THEY ARE NOT MAKING ANY PROMISES ABOUT UNKNOWN ALGORITHMS?

A. I CAN SEE WHERE YOU WOULD INTERPRET THAT WAY. BUT IF YOU DID, I DON'T KNOW WHAT THEY WOULD MEAN BY "DEMONSTRABLY INFEASIBLE."

Q. IF THE FASTEST KNOWN ALGORITHM TAKES TEN TO THE 30TH OPERATIONS, ISN'T THAT DEMONSTRABLY INFEASIBLE, SIR?

A. WELL, WHAT IS BEING DEMONSTRATED, THOUGH?

THE COURT: WHICH COLUMN ARE WE ON NOW?

MR. FLINN: IT'S COLUMN TWO, YOUR HONOR, LINE 43, IN WHICH --

THE COURT: I HAVE IT. I HAVE IT.

"PUBLICLY KNOWN TRANSMISSION OF THE MESSAGE SENT BY..."

MR. FLINN: YES. OH. IT'S 43: THE ILLUSTRATED EMBODIMENT DIFFERS FROM PRIOR APPROACHES TO A PUBLIC KEY

CRYPTOSYSTEM IN THAT IT, MEANING THE SYSTEM HERE, IS PRACTICAL TO IMPLEMENT AND DEMONSTRABLY INFEASIBLE USING KNOWN METHODS.

Q. YOU RECALL THE TESTIMONY YESTERDAY ABOUT THE PROOF OF IMPOSSIBILITY AND THE ONE-TIME PAD BEING THE ONLY CRYPTOSYSTEM THAT COULD BE PROVEN TO BE IMPOSSIBLE TO BREAK? DO YOU RECALL THAT TESTIMONY?

A. YES.

Q. DO YOU AGREE WITH IT?

MR. FRAM: OBJECTION, YOUR HONOR, VAGUE. I, FRANKLY, DON'T KNOW WHAT TESTIMONY MR. FLINN'S REFERRING TO.

MR. FLINN: I'LL WITHDRAW THE QUESTION AND BE MORE PRECISE.

Q. DO YOU AGREE WITH THE PROPOSITION THAT THE ONLY PROVEN CRYPTOSYSTEM TO BE IMPOSSIBLE TO BREAK IS THE ONE-TIME PAD SYSTEM?

A. THE TESTIMONY YESTERDAY MAY HAVE SAID IT A LITTLE MORE ACCURATELY.

THE ONLY -- THE ONLY KNOWN SYSTEM WHICH IS -- OFFERS SOME UNCONDITIONAL SECURITY AND PROOF OF UNBREAKABILITY IS THE ONE-TIME PAD AND VARIANCE OF IT. I THINK THERE PROBABLY ARE SOME OTHER CRYPTOSYSTEMS THAT MAY BE PROVEN UNBREAKABLE UNDER VARIOUS OTHER ASSUMPTIONS.

Q. YOU'D AGREE WITH ME THAT NO ONE, IN 1977, HAD PROVED

OR EVEN PURPORTED TO PROVE THAT TRAP DOOR KNAPSACKS WERE IMPOSSIBLE TO BREAK?

A. IN 1977? I WOULD AGREE WITH THAT. BUT IN THE CONTEXT OF THE SPECIFICATION, I WOULD SAY "PROVE" AND "DEMONSTRATE" MEAN SLIGHTLY DIFFERENT THINGS.

I MEAN, IF THE INVENTORS HAD USED THE WORD "PROVE" HERE, I WOULD TAKE THAT TO BE PROVED IN A MATHEMATICAL SENSE. IF THEY SAID "DEMONSTRATE," I WOULD INTERPRET THAT AS SOME WEAKER, SCIENTIFIC SENSE.

Q. WOULD YOU RETURN TO COLUMN FIVE AGAIN, THE PARAGRAPH BEGINNING AT LINE 15? YES.

DO YOU SEE THE PHRASE THERE, BEGINNING "THEORY SUGGESTS THE DIFFICULTY OF THE KNAPSACK PROBLEM"? DO YOU SEE THAT?

A. YES.

Q. THAT'S PRETTY DIFFERENT LANGUAGE THAN "THEORY PROVES." ONCE YOU'VE PROVEN IT, IT'S NO LONGER A THEORY; IS IT?

A. THAT'S CORRECT. THAT'S CORRECT. BUT --

Q. I'VE GOT ANOTHER QUESTION FOR YOU, ABOUT WHY IT IS NEW ALGORITHMS CAN BREAK CODES THAT COULDN'T BE BROKEN BEFORE.

WOULD YOU AGREE WITH ME THAT NEW ALGORITHMS CAN BREAK CODES THAT COULDN'T BE BROKEN BEFORE BECAUSE THE ALGORITHMS REDUCE THE NUMBER OF OPERATIONS IT TAKES OR CAN REDUCE THE NUMBER OF OPERATIONS IT TAKES IN ORDER TO GUESS OR BREAK THE CODE?

A. I WOULDN'T AGREE THAT NEW ALGORITHMS CAN BREAK CODES THAT COULDN'T BE BROKEN BEFORE.

Q. THAT'S NOT MY QUESTION.

THE REASON WHY A NEW ALGORITHM CAN BREAK A PREVIOUSLY UNBREAKABLE CODE IS BECAUSE THE ALGORITHM CAN REDUCE THE NUMBER OF OPERATIONS IT TAKES IN ORDER TO LEARN THE CODE?

A. I DON'T AGREE WITH YOUR PREMISE.

Q. DID THE ALGORITHM PUBLISHED BY DR. SHAMIR IN 1982, THAT BROKE THE SIMPLE VERSION OF KNAPSACKS, REDUCE THE NUMBER OF OPERATIONS THAT IT TOOK BEYOND WHAT HAD BEEN KNOWN BEFORE?

A. YES.

Q. NOW, LET'S LOOK BACK UP HERE AT THE TOP OF COLUMN FIVE, THE LANGUAGE WE'VE BLOWN UP. AND YOU'LL SEE THAT WE BEGIN OUR BLOWUP WITH THE WORDS "TO THE KNAPSACK PROBLEM" IN BRACKETS. THAT'S ACTUALLY, OF COURSE, NOT IN THE ACTUAL TEXT.

BUT YOU'D AGREE WITH ME THAT THE SOLUTION THAT THEY'RE TALKING ABOUT IS A SOLUTION TO THE KNAPSACK PROBLEM?

A. I'M SORRY. I DON'T SEE THE BRACKETS.

Q. DO YOU SEE THE FIRST LINE, "A SUPPOSED SOLUTION"?

A. OH, YES, YES.

Q. DO YOU SEE THE WORDS IN BRACKETS, "TO THE KNAPSACK

PROBLEM"?

A. YES.

Q. AND IF YOU LOOK IN THE ACTUAL TEXT OF THE PATENT, THOSE WORDS DON'T APPEAR THERE. BUT TO PUT THEM IN CONTEXT, WOULD YOU AGREE WITH ME THAT IT'S FAIR TO SAY THAT WHAT THEY'RE TALKING ABOUT IS A SOLUTION TO THE KNAPSACK PROBLEM?

A. YES.

Q. OKAY.

A. BUT -- ACTUALLY, LET ME -- I'M NOT SURE IF IT'S REFERRING TO THE KNAPSACK OR THE TRAP DOOR KNAPSACK. LET ME CHECK.

YES, I'D SAY IT REFERS TO THE KNAPSACK PROBLEM.

Q. OKAY. THE NEXT CLAUSE REFERS TO CHECKED IN AT MOST N ADDITIONS. IS THAT THE NUMBER OF OPERATIONS WE'RE REFERRING TO? "N" IS THE NUMBER OF OPERATIONS?

A. "N" IS DEFINED AS THE NUMBER OF LENGTHS IN THE KNAPSACK. IT THEN OCCURS IN THAT SENTENCE AS THE NUMBER OF OPERATIONS, YES.

Q. AND THEN THE NEXT CAUSE SAYS: "BUT TO THE BEST OF CURRENT KNOWLEDGE."

YOU'D AGREE WITH ME THAT THAT WOULD INCLUDE CURRENTLY KNOWN ALGORITHMS?

A. BUT CURRENTLY KNOWN ALGORITHMS AS APPLIED TO THIS PROBLEM, YES.

Q. AND THE NEXT SENTENCE SAYS: "EXHAUSTIVE TRIAL AND ERROR SEARCH OVER ALL TWO TO THE N POSSIBLE X'S IS COMPUTATIONALLY INFEASIBLE IF N IS LARGER THAN ONE OR 200."

DO YOU SEE THAT, SIR?

A. YES.

Q. NOW, IN THAT SENTENCE, THE USE OF THE WORD "COMPUTATIONALLY INFEASIBLE" IN THAT SENTENCE IS NOT TRUE, IF ONE APPLIES YOUR DEFINITION TO THIS SENTENCE; ISN'T THAT RIGHT?

A. NO, I DON'T THINK IT IS RIGHT.

Q. YOU'D AGREE WITH ME THAT NO ONE HAS PROVED THAT THERE IS NO ALGORITHM THAT CAN BREAK KNAPSACKS IN FEWER THAN TWO TO THE N OPERATIONS?

A. THAT'S NOT WHAT IT SAYS.

Q. LET ME REPHRASE THE QUESTION.

YOU WOULD AGREE WITH ME THAT IT IS THEORETICALLY POSSIBLE THAT TOMORROW, OR NEXT MONTH OR NEXT YEAR, SOME BRIGHT MATHEMATICIAN IS GOING TO INVENT A WAY TO SOLVE THE KNAPSACK PROBLEM FASTER THAN WAS KNOWN IN 1977?

A. YES.

Q. OKAY. BUT THAT THERE MIGHT BE SOME UNKNOWN ALGORITHM THAT COULD BREAK THE KNAPSACK; ISN'T THAT RIGHT?

A. YES.

Q. BUT YOUR DEFINITION OF "COMPUTATIONALLY INFEASIBLE"

REQUIRES, TO BE COMPUTATIONALLY INFEASIBLE, WE MUST BE PROTECTED AGAINST 1977-ERA EQUIPMENT, BUT KNOWN AND UNKNOWN ALGORITHMS; RIGHT?

A. YES.

Q. SO, THE KNAPSACK PROBLEM DOES NOT MEET YOUR DEFINITION OF "COMPUTATIONALLY INFEASIBLE"; DOES IT?

A. THE TRAP DOOR KNAPSACK?

Q. THAT'S RIGHT. NO, EXCUSE ME. THE KNAPSACK PROBLEM DOES NOT MEET YOUR DEFINITION OF "COMPUTATIONALLY INFEASIBLE"?

A. NO, I DON'T AGREE WITH THAT.

Q. YOU JUST TOLD US THAT IN ORDER TO MEET THE DEFINITION, IT HAS TO BE SECURE AGAINST UNKNOWN ALGORITHMS, AND YOU TOLD US THAT SOMEBODY MIGHT INVENT AN ALGORITHM TO BREAK KNAPSACKS.

HOW CAN IT MEET YOUR DEFINITION OF "COMPUTATIONALLY INFEASIBLE" IF SOME UNKNOWN ALGORITHM COULD BREAK IT AT SOME LATER TIME?

A. WELL, I THINK IT'S ALSO POSSIBLE THAT NO ALGORITHM -- WELL, FIRST OF ALL, LET'S DISTINGUISH THE KNAPSACK AND THE TRAP DOOR KNAPSACK.

BY THE KNAPSACK, I REFER TO THE PROBLEM -- I REFER TO WHAT'S DEFINED AS THE KNAPSACK PROBLEM IN THE PREVIOUS PARAGRAPH IN THE SPECIFICATION, AS BEING THE GENERAL PROBLEM OF PUTTING BOXES IN A KNAPSACK, OR HOWEVER

YOU WANT TO DEFINE IT, AND THE TRAP DOOR KNAPSACK BEING THE CRYPTOSYSTEMS THAT'S DISCLOSED IN THE HELLMAN-MERKLE SPECIFICATION.

SO NOW IS YOUR QUESTION ABOUT THE KNAPSACK PROBLEM OR ABOUT THE TRAP DOOR KNAPSACK PROBLEM?

Q. MY QUESTION IS ABOUT THE KNAPSACK PROBLEM, AND IT IS THIS: YOU PREVIOUSLY TESTIFIED THAT THERE MAY BE AS YET UNKNOWN ALGORITHMS THAT COULD BREAK THE KNAPSACK PROBLEM. AND YOU TOLD US THAT PROTECTION AGAINST THAT IS ONE OF THE ELEMENTS OF COMPUTATIONALLY INFEASIBLE.

SO DOESN'T IT NECESSARILY FOLLOW THAT THE KNAPSACK PROBLEM DOES NOT MEET YOUR DEFINITION OF "COMPUTATIONALLY INFEASIBLE"?

A. I'D SAY IT'S AN UNKNOWN PROBLEM IN COMPUTER SCIENCE, WHETHER OR NOT THE KNAPSACK PROBLEM IS COMPUTATIONALLY INFEASIBLE.

Q. WAS IT AN UNKNOWN PROBLEM IN 1977, WHETHER THE TRAP DOOR KNAPSACK PROBLEM WAS COMPUTATIONALLY INFEASIBLE?

A. IT WAS -- YES, THAT'S CORRECT; IT WAS NOT KNOWN TO THE INVENTORS AND TO LEADING EXPERTS, AS FAR AS ANYBODY HERE KNOWS, WHETHER OR NOT THE TRAP DOOR KNAPSACK WAS COMPUTATIONALLY INFEASIBLE IN 1977.

Q. IN YOUR OPINION, IN 1977 -- STRIKE THAT.

YOU'VE GOT YOUR OWN PATENTS; DON'T YOU?

A. YES.

Q. AND YOU'RE ADMITTED TO THE U.S. PATENT BAR; AREN'T YOU?

A. YES.

Q. SO YOU'RE PRETTY FAMILIAR WITH HOW PATENTS ARE PROSECUTED AND OBTAINED?

A. YES.

Q. AND ARE YOU FAMILIAR WITH THE PROPOSITION THAT A INVENTOR CAN BE HIS OR HER OWN LEXICOGRAPHER?

A. YES.

Q. THAT THE INVENTOR IS FREE TO DEFINE THE TERMS IN A PATENT CLAIM HOWEVER HE OR SHE WANTS; ISN'T THAT RIGHT?

A. YES.

Q. SO THE INVENTORS HERE WERE ALLOWED TO COME UP WITH THEIR OWN DEFINITION OF "COMPUTATIONALLY INFEASIBLE"; IS THAT RIGHT?

A. YES.

MR. FRAM: OBJECTION, YOUR HONOR. I BELIEVE THE LAST QUESTION JUST CROSSED THE LINE TO ASKING THE WITNESS TO APPLY HIS UNDERSTANDING OF PATENT LAW AS A MEMBER OF THE PATENT BAR.

THE COURT: YES.

MR. FRAM: I BELIEVE WE'VE GOT SOME SUBSTANTIAL BRIEFS FROM DEFENDANT SUGGESTING THAT'S NOT THE WAY TO GO.

MR. FLINN: I'LL WITHDRAW THE QUESTION AND REPHRASE IT THIS WAY:

Q. LET ME ASK YOU TO ASSUME, FOR PURPOSES OF MY QUESTIONS, THAT DR. HELLMAN AND DR. MERKLE WERE FREE TO DEFINE "COMPUTATIONALLY INFEASIBLE" IN AT LEAST SOME REASONABLE MANNER.

DO YOU BELIEVE IT WOULD BE REASONABLE FOR THEM TO DEFINE "COMPUTATIONALLY INFEASIBLE" IN A WAY THAT THEY KNEW THEIR EMBODIMENT DID NOT FULFILL THE DEFINITION?

A. NO. IF THE INVENTORS KNEW THAT THEIR OWN DEFINITION FAILED THE DEFINITION, THEN THAT WOULD NOT BE REASONABLE, BUT I'M SURE THE INVENTORS DID NOT KNOW.

Q. THE INVENTORS KNEW, AT LEAST ACCEPTED THE POSSIBILITY, DIDN'T THEY, THAT SOMEONE MIGHT SOMEDAY INVENT AN ALGORITHM THAT WOULD REDUCE THE NUMBER OF OPERATIONS IT TOOK TO BREAK THE TRAP DOOR KNAPSACK; ISN'T THAT RIGHT?

THE COURT: I THINK IT GOES PRETTY FAR FROM THE POINT.

MR. FLINN: I'LL --

THE COURT: DO YOU WANT TO TAKE A RECESS AND THINK ABOUT IT AND WRAP IT UP IN ANOTHER HALF HOUR?

MR. FLINN: I HAD JUST ONE LINE OF QUESTIONING. IF IT'S AN APPROPRIATE TIME TO TAKE A BREAK, IT'S A NEW SUBJECT. THAT WOULD BE FINE.

THE COURT: HOW LONG ARE YOU GOING TO BE WITH THE WITNESS?

MR. FLINN: ANOTHER TEN MINUTES.

THE COURT: FIVE?

MR. FLINN: FIVE MINUTES; THAT'S FINE.

THE COURT: OKAY. EXCUSE ME.

MR. FLINN: OH, I'M SORRY. I THOUGHT WE WERE TAKING A RECESS NOW.

Q. I WANT TO ASK YOU ABOUT AUTHENTICATION.

THE COURT: THEN YOU CAN REDIRECT YOURSELF AFTERWARDS.

THE WITNESS: YEAH, YEAH. WELL, ACTUALLY, I DO HAVE SOME THINGS TO RESPOND TO, BUT I DON'T KNOW WHETHER TO --

THE COURT: LET HIM FINISH THE CROSS, AND THEN YOU CAN CONTINUE YOUR TESTIMONY, FROM WHAT HE RAISED, AND YOU CAN RESPOND TO IT.

MR. FLINN: Q. DO YOU RECALL DR. KONHEIM'S TESTIMONY ABOUT AUTHENTICATION YESTERDAY; DO YOU?

A. YES.

Q. RATHER THAN CHARACTERIZING IT MYSELF AND MAKING AN ERROR FOR SOMETHING THIS TECHNICAL, CAN YOU BRIEFLY GIVE US YOUR UNDERSTANDING OF WHAT HIS TESTIMONY WAS ON THAT SUBJECT?

THE COURT: THE SUBJECT --

MR. FLINN: OF THE AUTHENTICATION QUESTION AND PROVING IDENTITY.

THE COURT: GO AHEAD.

THE WITNESS: I'M SURPRISED I'M NOT HEARING AN OBJECTION ON THAT, BUT --

MR. FRAM: PERHAPS MR. FLINN WOULD LIKE TO FOCUS THE AREA OF THE AUTHENTICATION TESTIMONY? IF NOT, OBJECTION, OVERBROAD.

THE COURT: YES, OKAY.

MR. FLINN: Q. DO YOU RECALL HIS TESTIMONY ABOUT YOUR REQUIREMENT FOR SOME IDENTITY PROOF ATTACHING, LIKE THROUGH A DRIVER'S LICENSE OR SOME OTHER MECHANISM, ATTACHING SOME ADDITIONAL PROOF TO POSSESSION OF A SECRET KEY? IS THAT MORE SPECIFIC FOR YOU, SIR?

A. WELL, DO YOU WANT ME TO CHARACTERIZE WHAT HE SAID?

Q. VERY BRIEFLY, BECAUSE I'VE GOT SOME --

A. I MEAN, YOU KNOW, HE BELIEVED YOU IDENTIFY PEOPLE WITH DRIVERS' LICENSES. THAT'S THE WAY HIS GROCERY STORE IDENTIFIES HIM AND...

Q. DO YOU BELIEVE THAT IS AN ESSENTIAL REQUIREMENT FOR AUTHENTICATION IN A PUBLIC KEY SYSTEM?

A. DRIVERS' LICENSES?

Q. YES.

A. ESSENTIAL? NO. I THINK THERE ARE LOTS OF WAYS OF IDENTIFYING PEOPLE.

Q. ISN'T IT COMMON, IN A WIDE RANGE OF COMPUTER-RELATED ACTIVITIES, THAT PEOPLE ARE IDENTIFIED OR AUTHENTICATED MERELY BY POSSESSION OF SOME KEY OR PASSWORD?

A. WELL, OKAY, I'LL SEE IF I CAN ANSWER WHAT YOU'RE GETTING AT HERE.

PROFESSOR KONHEIM TESTIFIED, WITH REGARD TO THE CLAIM 2 OF THE HELLMAN-MERKLE PATENT AND THE CLAUSE THAT REFERS TO RECEIVING -- AUTHENTICATING THE RECEIVER'S IDENTITY.

AND AS I UNDERSTAND HIS TESTIMONY, HE SAID THAT THE AUTHENTICATION THAT THE HELLMAN-MERKLE PATENT IS AIMING AT IS THE AUTHENTICATION -- IS THAT OF LINKING THE RECEIVER TO THE POSSESSOR OF THE SECRET KEY. AND THAT -- AND THAT HIS OPINION THAT LINKING THE RECEIVER TO BEING -- TO THE POSSESSOR OF THE SECRET KEY IS NOT TRULY AUTHENTICATING THE RECEIVER UNLESS YOU HAVE A DRIVER'S LICENSE OR SOME OTHER PROOF OF THE PERSON'S IDENTITY.

Q. LET ME ASK IT THIS WAY.

YOU'RE FAMILIAR WITH THE VERY ROUTINE AND COMMON PROCEDURE WHEREBY PEOPLE LOG ONTO COMPUTERS OR COMPUTER NETWORKS?

A. YES.

Q. AND THEY DO THAT BY ENTERING A PASSWORD?

A. YES.

Q. AND UPON VERIFICATION OF THE PASSWORD, THE COMPUTER ALLOWS THE USER ACCESS TO RESOURCES INSIDE THE COMPUTER NETWORK; IS THAT RIGHT?

A. YES.

Q. HAVE YOU EVER SEEN A COMPUTER, IN THE AVERAGE SYSTEM, ASK FOR SOMEONE'S DRIVER'S LICENSE?

A. NO, BUT I WOULD SAY IT'S SOMETIMES THE CASE THAT WHEN YOU SET UP THE COMPUTER ACCOUNT AND YOU GO MEET SOME ADMINISTRATORS OR CLERKS TO SET UP THE ACCOUNT, THAT YOU MIGHT HAVE TO PRESENT SOME IDENTIFICATION AT THAT TIME, AND YOU MIGHT HAVE TO PRESENT A DRIVER'S LICENSE AT THAT TIME.

AND IF THE COMPUTER SYSTEM MANAGEMENT HAS REQUIRED DRIVER'S LICENSES OF ALL THEIR USERS AT ONE TIME AND MADE RECORDS OF THAT IN THEIR BOOKS, THEN YOU COULD VIEW ENTERING THAT PASSWORD ON THE COMPUTER SYSTEM AS, IN SOME SENSE, A VERIFICATION OF THAT PERSON'S DRIVER'S LICENSE, BECAUSE THE DRIVER'S LICENSE AND THE PASSWORD WERE LINKED AT THE TIME OF THE ACCOUNT SETUP.

Q. BUT SOMEONE ELSE COULD HAVE GOTTEN THE PASSWORD AT ANY TIME THEREAFTER; ISN'T THAT RIGHT?

A. IF THAT USER WERE TO GIVE OUT HIS PASSWORD TO OTHERS, IT WOULD DEFEAT SOME OF THE PURPOSE OF THE AUTHENTICATION, YES.

THE COURT: AUTHENTICATION IS SOMETHING, IS IT NOT? YOU RECEIVE A MESSAGE AND YOU WANT TO AUTHENTICATE THE SENDER; IT'S ALMOST IMMEDIATE, OR VICE-VERSA?

THE WITNESS: USUALLY, BUT THERE MIGHT BE SOME DELAY.

BUT YEAH, TO DEFEAT THE SYSTEM, JUST AS IF YOU GAVE OUT YOUR, YOU KNOW, YOUR DRIVER'S LICENSE TO SOMEBODY, THAT WOULD DEFEAT THE PURPOSE OF USING DRIVER'S LICENSE AS AUTHENTICATION.

MR. FLINN: Q. UNLESS YOU WERE THE BEST LOOKING PERSON IN THE WORLD.

I'M SORRY. I WITHDRAW THE QUESTION. I'M DONE. THANK YOU.

THE COURT: OKAY.

MR. KRAMER: YOUR HONOR, I JUST HAVE ONE OR TWO QUESTIONS I WANT TO FOLLOW UP BECAUSE THE WITNESS SAID SOMETHING VERY SURPRISING TO ME.

MR. FRAM: YOUR HONOR, IF DEFENDANTS WANT TO KEEP GANG-TACKLING WITNESSES, I SUPPOSE THAT'S THEIR PREROGATIVE --

MR. KRAMER: IF --

MR. FRAM: IF I COULD, MR. KRAMER, I'M SURE HE HAS NEW QUESTIONS, YOUR HONOR. THAT'S NOT OUR CONCERN. IT'S SIMPLY THE FACT THAT THEY ARE CLEARLY PRESENTING JOINT SUBMISSIONS.

MR. KRAMER REPRESENTS STANFORD; MR. FLINN REPRESENTS CARO-KANN; MR. KENNEDY REPRESENTS CKC. I'M SURE MS. GOLD REPRESENTS ALL OF THEM. BUT THEY CHOOSE NOW TO WEAR VARIOUS HATS BECAUSE THEY WANT TO HAVE A STREAM OF LAWYERS EXAMINING WITNESSES.

WE DID IT YESTERDAY WITH THE OTHER WITNESSES. NOW WE'RE DOING IT WITH MR. SCHLAFLY. WE THINK IT'S REALLY CROSSING THE LINE.

THE COURT: THAT WILL BE THE RULE FROM HENCEFORTH.

MR. KRAMER: YOUR HONOR --

THE COURT: BUT FROM NOW ON, ONE ATTORNEY DOES THE EXAMINATION FOR A PARTY.

MR. KRAMER: I'LL MAKE AN OFFER OF PROOF, IF THE COURT IS INTERESTED.

THE COURT: I'LL ACCEPT YOUR WORD THAT IT'S IMPORTANT, BUT THE PROCEDURE IS THAT WE'LL HAVE ONE LAWYER REPRESENT THE CLIENT FOR CROSS-EXAMINING OF THE WITNESS, SO WE DON'T HAVE THREE LAWYERS EXAMINING THE SAME WITNESS FOR THE SAME CLIENT.

CROSS-EXAMINATION

BY MR. KRAMER: Q. MR. SCHLAFLY, YOU SAID SOMETHING THAT SURPRISED ME ABOUT DR. KNUTH'S BOOK. YOU AND I HAD A CONVERSATION ABOUT THIS VERY BOOK AND DR. KNUTH AFTER PROFESSOR KONHEIM'S DEPOSITION. DO YOU RECALL THAT? DO YOU RECALL TELLING ME THAT DR. KNUTH WROTE THE BIBLE IN COMPUTER SCIENCE?

A. NO, BUT I'LL TAKE YOUR WORD FOR IT.

Q. SO YOU'RE NOT DENYING THAT WE HAD THAT CONVERSATION; CORRECT?

A. NO. IF YOU -- --

Q. IT IS COMMONLY --

A. NO.

Q. IT IS COMMON -- EXCUSE ME.

THE COURT: EVEN THE BIBLE HAS FLAWS.

MR. KRAMER: UNDERSTOOD.

THE WITNESS: IF YOU ASK ME WHETHER OR NOT THAT BOOK IS THE BIBLE, GO AHEAD AND ASK IT.

MR. KRAMER: Q. IS THIS BOOK COMMONLY KNOWN AS THE BIBLE IN COMPUTER SCIENCE?

THE COURT: AT WHAT TIME?

MR. KRAMER: PRESENTLY, SINCE IT WAS PUBLISHED.

THE WITNESS: THAT BOOK IS THE MOST AUTHORITATIVE BOOK ON THE SUBJECT.

MR. KRAMER: THANK YOU.

THE WITNESS: I'LL GRANT YOU THAT. HOWEVER, I DON'T THINK THAT CONTRADICTS WHAT I SAID.

FLINN ASKED ME A QUESTION ABOUT WHETHER KNUTH WAS ONE OF THE LEADERS IN COMPLEXITY THEORY, AND THAT'S A DIFFERENT QUESTION.

THE COURT: THANK YOU VERY MUCH. WE'LL RECESS FOR 15 MINUTES.

(RECESS TAKEN AT 11:05 A.M.)

(PROCEEDINGS RESUMED AT 11:22 A.M.)

MR. FRAM: YOUR HONOR?

THE COURT: YES, SIR?

MR. FRAM: RSA HAS A FEW QUESTIONS, IN LIGHT OF THE RATHER EXTENSIVE CROSS ON THE TOPICS RAISED IN THAT CROSS-EXAMINATION.

THE COURT: FINE.

MR. FRAM: I'LL TRY AND KEEP IT BRIEF, IN LIGHT OF THE TIME.

THE COURT: PARDON ME?

MR. FRAM: WE'LL TRY AND KEEP IT BRIEF, IN LIGHT OF THE TIME.

THE COURT: THANK YOU.

CROSS-EXAMINATION

BY MR. FRAM: Q. MR. SCHLAFLY, I THINK YOU MENTIONED THAT THE BROAD CONCEPT OF THE PUBLIC KEY SYSTEM WAS IN THE PRIOR ART, AND YOU MENTIONED SOME ARTICLES. I BELIEVE THE MULTIUSER ARTICLE WAS ONE OF THEM?

A. YES.

Q. I'D LIKE TO DRAW YOUR ATTENTION TO THAT. IT'S BEEN MARKED AS PLAINTIFF'S EXHIBIT 1001. DO YOU HAVE A COPY UP THERE WITH YOU? IF NOT, I'D BE HAPPY TO GIVE YOU ONE.

A. IT'S NOT ON ME. I PROBABLY HAVE ONE AT MY TABLE.

MR. FRAM: WITH THE COURT'S PERMISSION?

THE COURT: YES.

MR. FRAM: Q. NOW, DURING THE EXAMINATION BY MR. FLINN, THERE WAS A DISCUSSION OF THE TERM "GENERATING"

IN THE CONCEPT OF GENERATING KEYS, GENERATING PUBLIC KEYS, SO FORTH. DO YOU RECALL THAT TESTIMONY, JUST BEFORE THE BREAK?

A. YES.

Q. AND I BELIEVE YOU TESTIFIED, AFTER SOME BACK AND FORTH, THAT, IN YOUR VIEW, THE TERM "GENERATING" DOES HAVE A MEANING IN THE ART OF CRYPTOGRAPHY. HAVE I MISCHARACTERIZED YOUR ANSWER?

A. NO.

Q. OKAY. I'D LIKE YOU TO TURN, IF YOU WOULD, PLEASE, TO THE MULTIUSER ARTICLE. THAT'S THE ARTICLE BY MR. DIFFIE AND PROFESSOR HELLMAN MARKED AS EXHIBIT 1001.

I'D LIKE YOU TO TURN TO THE DISCUSSION OF PUBLIC KEY CRYPTOGRAPHY THAT'S ON PAGE 110. IT'S THE SECOND PAGE HERE IN THE EXHIBIT. IN THE SECOND COLUMN, YOU'LL SEE THE HEADING ON PUBLIC KEY CRYPTOGRAPHY. DO YOU SEE THAT?

A. YES.

Q. AND YOU'LL SEE THAT IN THE FIRST PARAGRAPH, THERE IS A DISCUSSION OF A PAIR OF KEYS, E AND D, WITH E BEING THE ENCIPHERING KEY, AND D BEING THE DECIPHERING KEY. DO YOU SEE THAT PARAGRAPH?

A. YES.

Q. NOW, LOOKING TO THE NEXT PARAGRAPH, FIRST SENTENCE, DO YOU SEE THE SENTENCE THAT SAYS, "FOR REASONS OF SECURITY, GENERATION OF THIS E-D PAIR IS BEST DONE AT THE USER'S

TERMINAL, WHICH IS ASSUMED TO HAVE SOME COMPUTATIONAL POWER."

DO YOU SEE THAT?

A. YES.

Q. SO THERE IS A DISCUSSION THERE OF GENERATING ENCIPHERING AND DECIPHERING KEYS; IS THERE NOT?

A. YES.

Q. AND THIS IS THE DISCUSSION IN ONE OF THE PIECES OF THE PRIOR ART THAT YOU WERE REFERRING TO BEFORE, IS THAT CORRECT, THE GENERAL CONCEPT OF THE PUBLIC KEY INTO THE PRIOR ART; IS THAT RIGHT?

A. YES, YES. IT'S CITED AS PRIOR ART IN THE PATENT.

TO BE FAIR, IT'S WRITTEN BY DIFFIE AND HELLMAN. BUT, YES, IT DOES GO INTO PRIOR ART.

Q. OKAY. LOOKING AT THAT SENTENCE THAT I JUST READ TO YOU REGARDING THE GENERATION OF THE E-D PAIR, CAN YOU TELL, FROM READING THAT SENTENCE, HOW TO GENERATE A PUBLIC KEY?

A. NOT SPECIFICALLY, NO. I MEAN --

Q. IN FACT --

A. I MEAN --

Q. I THINK YOU ANSWERED MY --

A. OH, OKAY.

Q. GO AHEAD. IF YOU HAVE SOMETHING TO ADD TO YOUR ANSWER, THAT'S FINE. YOU HAVE ANSWERED THE QUESTION. BUT

IF YOU'VE GOT SOMETHING MORE, GO AHEAD.

I GUESS MY QUESTION IS --

A. I MEAN, I CAN'T TELL FROM READING THE HELLMAN-MERKLE CLAIM 1 OR CLAIM 6 EXACTLY HOW TO READ -- TO GENERATE THE PUBLIC/PRIVATE KEY EITHER. BOTH THAT CLAIM AND THIS PAPER BOTH TALK ABOUT THE GENERAL IDEA OF PUBLIC KEY CRYPTOGRAPHY WITHOUT GOING INTO SPECIFICS.

Q. AND, IN FACT, AT THE TIME THIS PAPER WAS WRITTEN, ITS AUTHORS DID NOT KNOW, ACTUALLY, HOW TO GENERATE A PUBLIC KEY; DID THEY?

A. WELL, YES AND NO. AT THE END OF THIS PAPER ARE -- IS DESCRIBED THREE HYPOTHETICAL PUBLIC KEY SYSTEMS.

Q. AND THOSE SYSTEMS ARE THEN CHARACTERIZED, AREN'T THEY, AT THE TOP OF PAGE 111, FIRST COLUMN? DO YOU SEE THAT?

A. "AT PRESENT, WE HAVE NEITHER A PROOF THAT PUBLIC KEY SYSTEMS EXIST, NOR A DEMONSTRATION SYSTEM."

Q. AND THEN THEY GO ON TO DISCUSS SOME SUGGESTED EXAMPLES. I THINK THOSE ARE THE ONES YOU WERE REFERRING TO JUST BEFORE; ISN'T THAT RIGHT?

A. YES.

Q. SO, IN FACT, WHEN THEY WROTE THIS PAPER, NOT ONLY DID THEY NOT KNOW HOW TO GENERATE A PUBLIC KEY, AS THEY SAY HERE, THEY DID NOT EVEN KNOW IF ONE EXISTED; ISN'T THAT RIGHT? AND THOSE ARE THEIR WORDS; ISN'T IT?

A. NO. I WOULD SAY, BASED ON THIS, THE INVENTORS WERE

PRETTY SURE ONE EXISTED. YOU KNOW, THEY WEREN'T SURE EXACTLY HOW TO BEST GO ABOUT IT, BUT THEY WERE PRETTY SURE THAT ONE EXISTED.

Q. BUT THEY HAD NO PROOF THAT ONE EXISTED?

A. THEY HAD NO -- THEY HAD NO PROOF THAT ONE EXISTED -- WELL, I'M NOT SURE TO THIS DAY THEY HAVE A PROOF THAT ONE EXISTS.

Q. DID THEY HAVE A WORKABLE SYSTEM OF PUBLIC KEYS AT THE TIME THEY PUBLISHED THIS PAPER? THEY CERTAINLY DIDN'T HAVE A DEMONSTRATION SYSTEM; DID THEY?

A. YOU MEAN --

Q. WE CAN MAYBE SIMPLIFY THIS. THEY DIDN'T HAVE A DEMONSTRATION SYSTEM; DID THEY? THEY SAID THEY DIDN'T, SO I TAKE IT THEY DIDN'T HAVE ONE THAT THEY WEREN'T TALKING ABOUT HERE, THAT YOU KNOW OF? DO YOU KNOW OF ANY DEMONSTRATION SYSTEM THEY HAD, GIVEN THEY SAID IN THEIR PAPER THEY DIDN'T HAVE ONE?

A. I HAVE TO INTERPRET THOSE TERMS VERY CAREFULLY. I MEAN, I WOULD SAY THAT THE PUBLIC KEY CONCEPT, THE ABSTRACT CONCEPT, IS DEMONSTRATED IN THIS PAPER.

Q. OKAY.

A. BUT IT'S NOT -- BUT A DEMONSTRATION SYSTEM, A SYSTEM THAT REALLY, REALLY, DEFINES ALL THE NITTY-GRITTY THAT YOU WOULD NEED A PATENT DISCLOSURE OR SOMETHING LIKE THAT, NO.

Q. OKAY. SO ONE CAN TALK ABOUT GENERATING PUBLIC KEY IN

THE ART WITHOUT HAVING A WORKABLE PUBLIC KEY SYSTEM?

A. YES.

Q. AND ONE CAN TALK ABOUT, IN THE ART, THE GENERAL IDEA OF PUBLIC KEY SYSTEMS WITHOUT NECESSARILY HAVING ONE THAT CONSTITUTES A WORKABLE DEMONSTRATION SYSTEM?

A. YES.

Q. SO, WHEN YOU SAY THERE IS A MEANING IN THE ART FOR GENERATING A PUBLIC KEY, I TAKE IT THAT'S A VERY BROAD TERM?

A. YES. WELL, THE HELLMAN-MERKLE CLAIMS ARE BROAD CLAIMS.

Q. AND, IN FACT, THAT BROAD CONCEPT OF GENERATING PUBLIC KEYS WAS ALREADY IN THE PRIOR ART, AND, IN FACT, IT'S IN THIS PAPER?

MR. FLINN: AT SOME POINT, YOUR HONOR, WE'RE GETTING INTO A VALIDITY ARGUMENT AND NOT --

MR. FRAM: I'M JUST TRYING TO UNDERSTAND WHAT THE WITNESS MEANS WHEN HE SAYS THAT THE TERM "GENERATING A PUBLIC KEY" HAS A MEANING IN THE ART. I WANT TO SEE WHERE HE PLACES THAT. I THINK HE SAID IT'S A BROAD CONCEPT.

Q. I THINK YOU WOULD AGREE IT WAS ALREADY IN THE PRIOR ART, BEING IN THIS PAPER; IS THAT RIGHT?

A. I WOULD SAY THE WHOLE CONCEPT OF PUBLIC KEY AND DIGITAL SIGNATURE ARE DESCRIBED IN THIS PAPER, TOGETHER WITH GENERATING KEYS AND ENCIPHERING. FOR THE MOST PART,

IT'S ALL DESCRIBED IN KIND OF A GENERAL WAY, BUT IT'S ALL DESCRIBED IN THE PAPER.

Q. TO THE DEGREE THE PATENT USES THE TERM "GENERATING A PUBLIC KEY," DOES IT USE IT THE SAME WAY AS IT'S IN THIS PAPER, OR DOES IT PROVIDE A NARROWER USAGE OF THE TERM?

A. WELL, YEAH, I THINK YOU'RE ASKING A LEGAL QUESTION NOW. I MEAN, THAT DEPENDS ON OUR 112, SECTION 6 --

Q. GIVEN WHAT YOU SAID, ISN'T IT THE CASE THAT THE ONLY THING THE PATENT ADDS TO THE TERM "GENERATING KEYS" IS THE REFERENCE TO THE TRAP DOOR KNAPSACK?

A. THE ONLY THING THE PATENT SPECIFICATION ADDS TO THIS PRIOR ART PAPER?

Q. THE ONLY THING THE PATENT ADDS TO THAT, THE CONCEPT OF GENERATING KEYS, THAT WASN'T ALREADY IN THE PRIOR ART IS THE FACT THAT AT LEAST THE PATENTEES THOUGHT YOU COULD DO IT WITH THE TRAP DOOR KNAPSACK SYSTEM?

A. YES.

Q. NOW, MOVING TO THE TOPIC OF THE KNAPSACK BRIEFLY. THERE WAS SOME DISCUSSION OF THE SECURITY OF THE KNAPSACK, AND TURNING YOUR ATTENTION TO THE BOARD THAT WAS PUT UP THERE. THERE WAS A LOT OF DISCUSSION ABOUT WHAT IT WOULD TAKE TO BREAK THE KNAPSACK. DO YOU RECALL THAT CONVERSATION AND TESTIMONY BEFORE THE BREAK?

A. MY TESTIMONY, YES.

Q. THE DISCUSSION, THOUGH, I TAKE IT, HAVING TO DO WITH

THE BREAKING OF A KNAPSACK PROBLEM, THAT'S SOMETHING DIFFERENT THAN BREAKING A TRAP DOOR KNAPSACK; ISN'T THAT RIGHT?

A. YES.

Q. AND, IN FACT, IT CAN BE THE CASE THAT, WHILE A KNAPSACK CAN REMAIN HARD AND UNBREAKABLE, ONE CAN BREAK A TRAP DOOR KNAPSACK SYSTEM BY FINDING OUT THE INFORMATION ABOUT THE TRAP DOOR; ISN'T THAT RIGHT?

A. YES. THE TRAP DOOR KNAPSACK IS A PARTICULAR KIND OF KNAPSACK.

SOME TRAP DOOR KNAPSACKS ARE EASY TO SOLVE, AND SOME ARE, AS FAR AS WE KNOW, DIFFICULT. THE TRAP DOOR KNAPSACK REPRESENTS A PARTICULAR KIND OF KNAPSACK, AND IT COULD BE BREAKABLE WITHOUT OTHER KINDS OF KNAPSACKS BEING BREAKABLE.

Q. SO IF THERE IS DISCUSSION IN THE PATENT ABOUT THE DIFFICULTY OF BREAKING A KNAPSACK PROBLEM, THAT DOESN'T NECESSARILY TELL US ANYTHING ABOUT THE DIFFICULTY OF BREAKING A TRAP DOOR KNAPSACK; DOES IT?

A. WELL, I WOULD SAY THE INVENTORS CLEARLY THOUGHT IT TOLD THEM SOMETHING. I MEAN, IT DIDN'T GIVE A CONCLUSIVE MATHEMATICAL PROOF.

Q. ALL I'M SUGGESTING IS THAT IF THE INVENTORS DESCRIBED WHAT THEY THOUGHT WERE SOME OF THE CHARACTERISTICS OF THE KNAPSACK AND WHAT MADE IT HARD TO BREAK, THAT DOESN'T

NECESSARILY CONSTITUTE A STATEMENT ABOUT WHAT THEY THOUGHT ABOUT THE TRAP DOOR WAS HARD TO BREAK?

A. BASED ON MY READING OF THE INVENTOR'S PAPER, THE INVENTORS THOUGHT -- CLEARLY THOUGHT THAT THE KNAPSACK PROBLEM BEING HARD TO BREAK, WOULD BE EVIDENCE TO SUGGEST THAT THE TRAP DOOR KNAPSACK MIGHT ALSO BE HARD TO BREAK.

Q. I'M NOT ASKING --

A. BUT IT IS NOT A CONCLUSIVELY LOGICALLY DRAWN INFERENCE, NO.

Q. I DIDN'T ASK THE QUESTION OF WHAT THEY ACTUALLY THOUGHT.

WHAT I ASKED, SIMPLY, IS: IF I PROVIDED YOU A WRITTEN STATEMENT AND SAY THIS TELLS ME ABOUT THE DIFFICULTY OF BREAKING A KNAPSACK, AND THAT'S ALL I TELL YOU, THE KNAPSACK PROBLEM, A HARD KNAPSACK PROBLEM, I HAVEN'T NECESSARILY GIVEN YOU ENOUGH INFORMATION, HAVE I, ABOUT WHETHER IT'S POSSIBLE TO BREAK A TRAP DOOR KNAPSACK SYSTEM?

A. NOT NECESSARILY.

Q. OKAY.

A. IF YOU COULD BREAK ALL KNAPSACK PROBLEMS, YOU COULD ALSO BREAK ALL TRAP DOOR KNAPSACK PROBLEMS. BUT IT'S POSSIBLE YOU COULD BREAK TRAP DOOR KNAPSACK PROBLEMS WITHOUT BREAKING OTHER KINDS OF KNAPSACKS.

Q. YES.

FINALLY, JUST A QUESTION ABOUT AUTHENTICATION. IF I WERE TO GET A HOLD OF MR. FLINN'S PASSWORD AND TYPE IT IN AT HIS LAW FIRM, AT THAT POINT, WOULD I HAVE AUTHENTICATED MYSELF AS BEING MR. FLINN?

A. IT WOULDN'T MAKE YOU MR. FLINN. I --

Q. LET ME PERHAPS REPHRASE THE QUESTION.

A. I DON'T KNOW. I MEAN, YOU COULD ASK THE SAME QUESTION: IF YOU STOLE MR. FLINN'S DRIVER'S LICENSE AND USED IT TO CASH A CHECK, WOULD YOU HAVE AUTHENTICATED YOURSELF AS MR. FLINN? AND, YOU KNOW, I WOULD SAY IT'S A SIMILAR ANSWER. I MEAN, YOU KNOW, YOU FOOLED SOMEBODY INTO THINKING YOU'RE MR. FLINN, MAYBE, BUT --

Q. SO, IN BOTH CASES, OF THE LICENSE THEFT OR IMPERSONATING SOMEONE, I, IN FACT, COULD TRY AND BREAK THE SYSTEM, AND PRETEND I WAS SOMEBODY ELSE.

IN FACT, IF I JUST SHOWED UP AT MR. FLINN'S LAW FIRM -- I'LL GIVE YOU A HYPOTHETICAL -- AND SAID, "I JUST WANT TO LOG IN AND PRETEND I'M SOMEBODY ON THEIR COMPUTER SYSTEM," IT'S YOUR UNDERSTANDING, I TAKE IT, FROM YOUR TESTIMONY BEFORE, THAT THAT ISN'T DONE? I'D HAVE TO GO TO HIS MIS DEPARTMENT AND SOMEHOW OR OTHER VERIFY THAT I COULD HAVE A PASSWORD TO BE WHO I AM?

A. IF YOU WANTED TO GET A NEW ACCOUNT, YOU'D PRESUMABLY HAVE TO GO TO THEIR MIS DEPARTMENT AND GET AN ACCOUNT AND A PASSWORD. IF YOU HAPPEN TO KNOW OR STEAL OR WHATEVER

SOMEONE'S PASSWORD, YOU COULD, HOWEVER, SHORTCUT THAT.

Q. ACCEPTING THAT MALFEASANCE IS ALWAYS POSSIBLE, AND PUTTING ASIDE THE QUESTION OF MALFEASANCE, THE SIMPLE QUESTION IS: IF I WANT TO AUTHENTICATE MYSELF ON A PASSWORD SYSTEM, I TAKE IT IN THE ORDINARY COURSE, I NEED TO GO THROUGH PROPER PROCEDURES AND IDENTIFY THAT I AM WHO I SAY I AM, AS PART OF USING THAT SYSTEM; ISN'T THAT RIGHT?

A. NORMALLY, YES. I'M SURE MR. FLINN'S LAW FIRM WOULD NOT GIVE YOU AN ACCOUNT ON THEIR COMPUTER SYSTEM UNLESS YOU PROVIDED SOME EVIDENCE OF WHO YOU ARE.

Q. AND WITHOUT GETTING INTO THE KIND OF EVIDENCE OR WHETHER A DRIVER'S LICENSE IS GOOD ENOUGH OR FINGERPRINTS OR DNA OR WHATEVER, I TAKE IT SOME NOTION THAT I HAVE TO, IN FACT, SHOW WHO I AM IS PART OF WHAT IT MEANS TO USE AN AUTHENTICATION SYSTEM?

A. THAT IS CERTAINLY A DESIRABLE ATTRIBUTE OF AN AUTHENTICATION SYSTEM, YES.

MR. FRAM: THANK YOU, YOUR HONOR. NO FURTHER QUESTIONS.

THE COURT: OKAY.

WELL, NOW YOU HAVE YOUR RESPONSE.

THE WITNESS: NOW I GET TO CROSS-EXAMINE MYSELF?

THE COURT: THAT'S RIGHT.

THE WITNESS: AND IT'S --

THE COURT: JUST ON MATTERS BROUGHT UP DURING THE CROSS-EXAMINATION THAT YOU HAVEN'T COVERED IS ALL.

REDIRECT TESTIMONY

THE WITNESS: OKAY. AND HERE'S WHERE IT GETS EVEN HARDER FOR ME TO DISTINGUISH BETWEEN THE LEGAL ARGUMENTS AND FACT ARGUMENTS, BUT I'LL TRY MY BEST.

OKAY. BUT I'LL GO OVER A FEW POINTS BRIEFLY. IF YOU THINK THEY'RE LEGAL, I'LL JUST SKIP OVER THEM OR SOMETHING.

OKAY. I WAS ASKED ABOUT EVIDENCE IN THE INVENTORS' WRITINGS ABOUT INTERPRETATIONS THAT I GAVE FOR THE TERM "COMPUTATIONAL INFEASIBLE." AND I GAVE A SENTENCE, ON COLUMN TWO, THAT USED THE PHRASE "DEMONSTRABLY INFEASIBLE TO INVERT USING KNOWN METHODS."

I'D LIKE TO ALSO SAY THAT I THINK IT'S EVIDENCE THAT THE INVENTORS USED -- WERE INTENDING TO USE COMPLEXITY THEORY AND TO APPLY TO THEIR NOTION OF PUBLIC KEY CRYPTOGRAPHY IS THAT IN THE DIFFIE-HELLMAN NEW DIRECTIONS PAPER, THEY HAVE A SECTION ON COMPLEXITY THEORY, AND THEY CLEARLY TALK ABOUT COMPLEXITY THEORY THERE.

OKAY. IF I INTERPRET THE WORD "METHODS" THE WAY MR. FLINN SEEMS TO WANT ME TO INTERPRET THE WORD "METHODS," THEN THE SENTENCE ON COLUMN TWO THAT SAYS, "DEMONSTRABLY INFEASIBLE TO INVERT USING KNOWN METHODS," I

FIND IT VERY HARD TO ASSIGN MEANING TO THAT.

IF THE STATEMENT IS, DEMONSTRABLY INFEASIBLE -- IF THAT SENTENCE IS TO BE INTERPRETED AS MEANING DEMONSTRABLY INFEASIBLE TO INVERT USING PUBLISHED ALGORITHMS, THEN JUST ABOUT ANY NEW METHOD WILL BE, BECAUSE ONCE YOU PUT OUT A NEW METHOD, IT'S UNLIKELY THAT THERE IS GOING TO BE A PUBLISHED ATTACK ON EXACTLY THAT METHOD. AND SO, ALMOST ANYTHING WOULD BE DEMONSTRABLY INFEASIBLE TO INVERT USING KNOWN METHODS.

SO, IF I USE THE INTERPRETATION OF "METHOD" THAT FLINN WANTED ME TO TAKE, I HAVE A HARD TIME MAKING SENSE OUT OF THAT PHRASE. I UNDERSTAND THAT'S A BIT LEGALISTIC AND ARGUMENTATIVE, BUT I'M SAYING IT NOW TO GIVE THEM A CHANCE TO CROSS-EXAMINE ME ON THAT POINT, IF THEY WANT TO.

OKAY. THE NEXT POINT I WANT TO MAKE IS THAT I WAS ASKED SOME QUESTIONS THAT TOUCHED ON WHAT IS PROVEN AND WHAT IS DEMONSTRATED AND WHAT IS KNOWN FOR A FACT. AND I THINK TO UNDERSTAND MY ANSWERS ON THAT, I COME FROM A MATHEMATICAL BACKGROUND WHERE "PROVE" MEANS SOMETHING VERY PRECISE. AND WHAT "PROVE" MEANS TO ME IS NOT -- IS NOT THE SAME AS WHAT "DEMONSTRATE," FOR THE PURPOSES OF OBTAINING A PATENT, WOULD BE. AND THOSE ARE DIFFERENT NOTIONS.

AND, YOU KNOW, WE CAN ARGUE THAT IN LEGAL ARGUMENTS. BUT I JUST WANT TO SAY I DRAW THAT

DISTINCTION.

AND WHEN YOU ASKED ME A QUESTION ABOUT THE WORD "PROOF," I USE IT IN THE SENSE OF A MATHEMATICAL PROOF. WHEN SOMEONE APPLIES TO THE PATENT OFFICE WITH SOME, YOU KNOW, DRUG THAT THEY PURPORT TO CURE SOME DISEASE, THEY DON'T HAVE A MATHEMATICAL PROOF THAT IT CURES THAT DISEASE. THEY HOPE TO HAVE SOME SORT OF DEMONSTRATION, THE STANDARDS OF WHICH ARE COMPLETELY DIFFERENT FROM MATHEMATICS.

OKAY. FINALLY, I WANT TO SAY SOME ADDITIONAL REMARKS ABOUT PKZIP ENCRYPTION. PKZIP HAS AN ENCRYPTION FEATURE IN IT WHICH, I ADMITTED THAT THERE WERE ATTACKS ON IT, WHICH ALLOW IT TO BE BROKEN UNDER CERTAIN CIRCUMSTANCES, AND WHICH LIMIT ITS USEFULNESS, ALTHOUGH I TESTIFIED IT DOESN'T MAKE IT TOTALLY USELESS.

AND I THINK I SHOULD ADD A COUPLE THINGS TO THAT. I MEAN, I THINK, FOR ONE THING, IT DOESN'T MAKE IT TOTALLY USELESS BECAUSE THE PRODUCT IS NOT REALLY PRIMARILY A DATA ENCRYPTION PRODUCT, IN THAT THERE ARE LOTS OF PRODUCTS ON THE MARKET THAT HAVE ENCRYPTION SYSTEMS IN IT WHICH ARE TOTALLY WEAK AND TOTALLY TRIVIAL TO BREAK, FROM A CRYPTO ANALYST'S POINT OF VIEW; AND YET, THOSE FEATURES REMAIN IN THOSE PRODUCTS.

AND I MENTION, FOR EXAMPLE, LOTUS 1-2-3, WORD PERFECT, MICROSOFT WORD. THERE ARE LOTS OF THESE

PRODUCTS WHERE THEY HAVE PASSWORD FEATURES THEY ENCRYPT, AND YET, THOSE ENCRYPTION FEATURES, FROM A CRYPTO ANALYST'S POINT, ARE -- THEY'RE EASILY BROKEN. AND YET, THEY'RE STILL IN THERE. AND IT'S THE ONLY REASON THEY HAVE SOME UTILITY IS BECAUSE ENCRYPTION IS NOT REALLY THE PURPOSE OF THOSE PRODUCTS.

PKZIP HAD AN ENCRYPTION FEATURE THAT HAD SOME VERY UNUSUAL DESIGN REQUIREMENTS IN THAT NAMELY, I DIDN'T WANT SOMETHING THAT WOULD BE AUTOMATICALLY BROKEN, SUCH AS THE ENCRYPTION PROGRAMS IN, I DON'T KNOW, LOTUS 1-2-3, FOR EXAMPLE.

AT THE SAME TIME, SINCE PKZIP WAS GOING TO BE PUT OUT AT SHAREWARE AND COPIED ANYWHERE IN THE WORLD, THERE WOULD HAVE BEEN SOME LEGAL PROBLEMS IF I USED A STRONG ENCRYPTION METHOD IN IT. AND AS A RESULT, THAT IS, THAT IF I PUT AN ENCRYPTION METHOD IN IT THAT THE -- THAT THE NSA COULDN'T BREAK, THEN I COULD CONCEIVABLY BE CHARGED WITH A CRIMINAL OFFENSE FOR BEING AN ACCESSORY TO EXPORTING A MUNITION.

AND I KNOW IT SOUNDS RIDICULOUS, BUT THERE ARE LAWS IN THAT AREA THAT I HAD TO WATCH OUT FOR. AND AS A RESULT, THE ENCRYPTION METHOD WAS NOT AS SECURE AS IT OTHERWISE WOULD BE.

THAT'S ALL.

THE COURT: THANK YOU.

MR. FLINN: SPEAKING NOW AS I MUST FOR ALL OF US, WE HAVE NO QUESTIONS.

THE COURT: ALL RIGHT. FINE. THANK YOU.

MR. FRAM: NOTHING FURTHER, YOUR HONOR.

THE COURT: OKAY. THANK YOU, MR. SCHLAFLY.

(WITNESS EXCUSED.)

THE COURT: NEXT?

MR. HASLAM: I THINK WE'RE AT THE POINT WHERE, IF THE COURT WISHES TO ENTERTAIN ARGUMENT NOW, WE'RE PREPARED TO ARGUE ON SOME OF THE POINTS. WE CAN DO IT, I WOULD SUGGEST, RATHER THAN START FOR TEN MINUTES OR SO, WE COME BACK AFTER LUNCH, OR IF THE COURT WOULD PREFER TO CONSIDER THE EVIDENCE AND HAVE US COME BACK AT ANOTHER TIME AND ARGUE, WE'RE PREPARED TO DO THAT.

THE COURT: WHY DON'T YOU COME BACK IN ABOUT AN HOUR AND A HALF. WE'LL DO SOME ARGUMENT, AND WE'LL SEE IF WE HAVE ANY QUESTIONS OR WE NEED FURTHER ARGUMENT.

WE WILL NOT BE IN SESSION TOMORROW, BUT WE MIGHT SET DATES FOR ADDITIONAL ARGUMENT OR PAPERS OR --

MR. HASLAM: WE CAN DO THAT AT THE COURT'S CONVENIENCE, AND I KNOW THAT THERE IS ONE MOTION THAT IS ON THE CALENDAR.

THE COURT: YES.

MR. HASLAM: SO I GUESS WE'LL COME BACK AT 1:30. WE CAN DO SOME ARGUMENT ON THE MARKMAN ISSUES, OR WOULD

YOU LIKE TO DEAL WITH THE REMAND MOTION FIRST?

THE COURT: LET'S DO THE REMAND MOTION FIRST.

MR. HASLAM: OKAY. SO WE'LL COME BACK AT 1:30?

THE COURT: 1:30.

MR. KENNEDY: YOUR HONOR?

THE COURT: YES.

MR. KENNEDY: ONE OTHER POINT, IF I MIGHT, BEFORE WE RECESS. I FIND MYSELF SOMEWHAT IN THE SAME POSITION OF WHEN YOUR FAVORITE BALL PLAYER GETS TRADED TO ANOTHER TEAM AND COMES HOME, WHO DO YOU ROOT FOR?

AS YOU KNOW, I'VE TRIED TO MAKE VERY CLEAR FROM WHEN WE STARTED YESTERDAY, PERHAPS EXCESSIVELY, THAT I DIDN'T FEEL EXPERT OR LIVE TESTIMONY WAS NECESSARY. I STILL FEEL THAT WAY. ON THE OTHER HAND, THERE HAVE BEEN A NUMBER OF REFERENCES TO, "LOOK AT THAT. THE INVENTOR IS SITTING RIGHT HERE IN THE COURTROOM," AND SUGGESTING THERE IS SOME FOUNT OF KNOWLEDGE THAT WOULD BE OF ASSISTANCE TO THE COURT.

THE COURT: WELL, THERE IS SOME TESTIMONY THAT'S BEEN OFFERED THAT I WOULDN'T ACCEPT AS BINDING ME. I'D LIKE TO HEAR OTHER PEOPLE'S VIEWS. I MAKE THE DECISION, AND I HEAR VARIOUS VIEWS AND VARIOUS ARGUMENTS THAT PEOPLE MAKE. I'M NOT BOUND BY THAT. I LIKE TO SEE WHAT BOTH THE VIEWS ARE AND HOW YOU DESCRIBE THEM AND SO FORTH, AND IT WILL HELP ME MAKE UP MY MIND.

BUT I BASICALLY, ON THE EXTRINSIC EVIDENCE AREA, THE EXTRINSIC EVIDENCE COMES IN JUST BECAUSE IT MIGHT BE HELPFUL TO ME, NOT BECAUSE I FEEL BOUND BY IT.

MR. KENNEDY: MY CONCERN IS: I WANT TO DO WHATEVER IS MOST HELPFUL TO THE COURT, NOT TO MAINTAIN THE PURITY OF MY POSITION.

IF THE COURT FEELS THAT HEARING FROM PROFESSOR HELLMAN WOULD BE OF ANY ASSISTANCE, WE WILL REQUEST PERMISSION TO CALL HIM, AT LEAST FOR EXAMINATION BY THE COURT.

THE COURT: HE SAID THINGS IN HIS PRESENTATION -- HE WASN'T UNDER OATH, THAT BUT I ACCEPTED AS TRUE, AND HE MIGHT WANT TO REPEAT SOME OF THAT. THAT'S SOMETHING ELSE, OR THERE MAY BE SOMETHING ELSE HE CAN ADD.

I KNOW THAT THE INVENTOR'S PURPOSES OR HIS THOUGHTS OF INTERPRETATIONS ARE NOT WHAT I GO ON. I GO FROM WHAT I READ AND EVERYONE ELSE READS IN THE PATENT.

SO THAT IT COULD BE HELPFUL. I DON'T FEEL THAT YOU SHOULD BE BOUND BY IT. IT MIGHT GIVE ME SOME MORE INSIGHT OR KNOWLEDGE THAT WOULD BE HELPFUL. THAT'S ALL.

MR. KENNEDY: WHATEVER YOUR HONOR'S PREFERENCE IS. IF YOU FEEL IT WOULD BE HELPFUL, I'LL FORMALLY REQUEST NOW, IF MR. HASLAM DOESN'T PUSH ME COMPLETELY AWAY FROM THE MICROPHONE, FOR LEAVE TO CALL MR. HELLMAN, AT LEAST TO GO INTO THE QUESTION OF WHAT WAS MEANT BY

"COMPUTATIONALLY INFEASIBLE," SINCE THAT SEEMED TO BE THE AREA, IN PARTICULAR --

THE COURT: WHAT HE MEANT OR WHAT HE CONSTRUES IT TO BE AS READ FROM THE DOCUMENT?

MR. KENNEDY: THE PROBLEM I HAVE IS I'M NOT SURE EITHER ONE OF THOSE IS GOING TO HELP YOU, SINCE IT SEEMS TO ME IT'S WHAT GOT WRITTEN RATHER THAN WHAT MAY HAVE BEEN INTENDED. THAT'S MY VIEW.

THE COURT: WHAT I INTERPRET FROM IT. BUT ANY INFORMATION THAT WOULD BE HELPFUL ABOUT THE INDUSTRY ITSELF AND HOW IT'S DEALT WITH --

MR. HASLAM: I JUST HAVE ONE COMMENT, AND I'M IN THE AWKWARD POSITION OF -- MR. KENNEDY WAS VERY CLEVER IN THE WAY HE DID THIS, IN INVITING THE COURT TO CALL HIS WITNESS. BUT WE HAVE RULES. AND I THINK THE COURT HAS SAID ANYTHING WE CAN AGREE ON, THE PARTIES, THE COURT WOULD BE WILLING TO DO. BUT WE DO HAVE A SET OF RULES.

TWICE, IN TWO DIFFERENT ORDERS, THE COURT SAID: IF YOU WANT TO CALL EXPERTS -- AND THAT'S WHAT HE'S JUST ASKED YOU TO DO, IS TO CALL EXPERTS -- TO DESIGNATE THEM.

WE DESIGNATED, BACK IN AUGUST, PROFESSOR KONHEIM. THEY DIDN'T DESIGNATE ANYONE. HAD THEY BEEN SURPRISED BY THAT, WHEN WE CONTINUED THE MARKMAN HEARING, WE HAD ANOTHER TIME AT WHICH WE COULD DESIGNATE IT. THEY THOUGHT WE HAD SURPRISED THEM BY DESIGNATING

PROFESSOR KONHEIM. THEY COULD HAVE DESIGNATED PROFESSOR HELLMAN AT THAT POINT IN TIME.

WE ASKED THEM AND WE HAVE BEEN ASKING THEM. AS LATE AS THIS MORNING BEFORE WE CAME HERE, WE SAID, "ARE YOU GOING TO PUT PROFESSOR HELLMAN ON THE STAND?"

AND THEY SAID "NO."

AND TO DO THIS NOW I THINK IS -- MY HAT IS OFF. I'VE LEARNED SOMETHING FROM MR. KENNEDY HERE TODAY. AND I RECOGNIZE THAT IF THE COURT ULTIMATELY THINKS THERE IS SOMETHING TO BE GAINED BY HAVING PROFESSOR HELLMAN COME ON THE STAND, THAT HE'S GOING TO DO IT. BUT I DO WANT TO REGISTER MY SHARP PROTEST, THAT THERE ARE RULES, AND WE ARE SETTING THE STAGE HERE FOR WHAT THE RULES ARE GOING TO BE THAT WE'RE GOING TO PLAY BY IN LATER HEARINGS AND TRIALS.

AND I THINK THAT THIS IS UNFAIR. IT SHOULD HAVE BEEN DONE BEFORE. THEY SHOULD HAVE TOLD US LAST NIGHT. THEY SHOULD HAVE TOLD US THIS MORNING. AND TO DO THIS AT THE 12TH HOUR I THINK IS JUST --

THE COURT: I THOUGHT THERE WAS A REQUEST. WASN'T THERE A REQUEST THE DAY BEFORE?

MR. KENNEDY: YES, YOUR HONOR. WE'VE TOLD THEM FROM THE VERY BEGINNING THAT WE INTENDED TO CALL PROFESSOR HELLMAN, NOT AS AN EXPERT, BUT AS A PERCIPIENT WITNESS. THEY'VE KNOWN ABOUT THAT FOR WEEKS.

I CONTINUE TO FEEL, WHETHER IT'S EXPERT OR PERCIPIENT, HE DOESN'T HAVE ANYTHING THAT'S GOING TO HELP THIS COURT INTERPRET A WRITTEN DOCUMENT. BUT I HAVE BEEN WRONG BEFORE. AND IF THE COURT FEELS OTHERWISE -- OBVIOUSLY, THE GOAL HERE IS NOT GAMESMANSHIP; IT'S TO GIVE THE COURT WHATEVER ASSISTANCE WOULD BE HELPFUL. IF THE COURT HAS QUESTIONS FOR PROFESSOR HELLMAN, HE'S HERE.

THE COURT: THANK YOU VERY MUCH.

NO, I BELIEVE THAT WE SHOULD HAVE RULES AND ENFORCE THEM, TOO. I AM NOT AS STRICT AS OTHERS. I'M GOING TO WEIGH THE PREJUDICE OF A MISTAKE, IF THAT'S WHAT IT WAS, AGAINST OPENING UP A LITTLE BIT AND NOT APPLYING THE RULES EXPLICITLY, BECAUSE SOMETIMES A PERSON CAN MAKE A MISTAKE, AND IT WOULD BE VERY PREJUDICE IN THE CASE NOT TO HAVE IT GO FORWARD.

IN THIS CASE, I DON'T THINK IT WOULD BE TERRIBLY PREJUDICIAL NOT TO HAVE MR. HELLMAN ON THE STAND. HE'S MADE A PRESENTATION WHICH IMPRESSED ME, AND I THINK I UNDERSTAND MUCH OF WHAT HE SAID. AND WHAT I DIDN'T UNDERSTAND, I'LL PROBABLY GET IT BEFORE THE CASE IS OVER.

BUT THE FEW THINGS THAT YOU THINK MIGHT BE HELPFUL TO ME, NOT GO THROUGH THE WHOLE ROUTINE AGAIN, I WOULD SAY THAT I WOULD BEND THE RULE. LET ME THINK ABOUT IT DURING THE RECESS. BECAUSE THERE MAY BE SOMETHING SPECIFIC HE COULD ASK HIM AND THEN LIMIT THAT RATHER THAN

A FULL BORE OR FULL RANGE OF CROSS-EXAMINATION.

MR. KENNEDY: THANK YOU, YOUR HONOR.

MR. SCHLAFLY: YOUR HONOR, I'D LIKE TO MAKE A SEPARATE OBJECTION --

THE COURT: ALL RIGHT.

MR. SCHLAFLY: -- WHICH YOU CAN THINK ABOUT.

I HAVE KIND OF MIXED VIEWS ON THIS BECAUSE I SIT HERE ON THE STAND SPECULATING ABOUT WHAT HELLMAN SAYS, AND IF THE PLAN WAS TO --

THE COURT: I VIEW IT AS SPECULATION. THAT'S THE WEIGHT I'LL GIVE IT.

MR. SCHLAFLY: AND OBVIOUSLY, HERE'S THE SOURCE RIGHT HERE.

ON THE OTHER HAND, I DEPOSED PROFESSOR HELLMAN ABOUT A YEAR AGO NOW. AND IN THAT DEPOSITION, I ASKED HIM VERY SPECIFIC QUESTIONS ABOUT WHAT HE MEANT BY "COMPUTATIONALLY INFEASIBLE" AND WHAT WAS MEANT AT THE TIME BY "COMPUTATIONALLY INFEASIBLE."

AND I GOT NOTHING OUT OF IT. I MEAN, HE EITHER SAID THAT HE DIDN'T REMEMBER, OR MR. FLINN, YOU KNOW, INSTRUCTED HIM NOT TO ANSWER. AND I GOT NOTHING OUT OF HIM ON THIS SUBJECT.

AND I WOULD HAVE LIKED TO HAVE HAD SOME ADVANCE NOTICE AS TO WHAT HE'S SAYING IN THE DEPOSITION, AND I THINK IT'S A LITTLE UNFAIR FOR HIM TO COME AND TESTIFY NOW

WHEN HE DIDN'T --

THE COURT: AND NOT BE ENLIGHTENED OF ME WHEN I ASKED THOSE QUESTIONS?

MR. SCHLAFLY: WELL, IF YOU WANT TO ASK HIM, GO AHEAD. I WOULD JUST LIKE TO SAY I THINK --

THE COURT: NO. IF THE WITNESS DOESN'T HAVE ANY KNOWLEDGE AT THE TIME AND THEN COMES UP AND ANSWERS LATER, THEN THEY CAN ALWAYS WONDER WHY AND ASK QUESTIONS OF HOW COME AT ONE TIME YOU COULDN'T REMEMBER OR COULDN'T ANSWER QUESTIONS AND NOW YOU CAN, IF THAT'S WHAT THE DEPOSITION ACTUALLY DEMONSTRATES.

MR. FLINN: YOUR HONOR, I WAS THERE AT THE DEPOSITION. I DEFENDED PROFESSOR HELLMAN.

THAT IS NOT WHAT HAPPENED AT THE DEPOSITION. AND THE SUGGESTION THAT SOMEHOW PROFESSOR HELLMAN FEIGNED SOME LACK OF RECALL IN THAT DEPOSITION, WHICH, AS I UNDERSTAND THE IMPORT OF MR. SCHLAFLY'S COMMENT, IS UNTRUE.

IF THAT WERE TRUE, HE HAD THE RECORD OF THE DEPOSITION. HE COULD HAVE BROUGHT IT AT THIS TIME. HE GOT THE DEPOSITION; THEY WERE THERE. THAT IS NOT A CORRECT CHARACTERIZATION, YOUR HONOR, OF WHAT HAPPENED AT THE DEPOSITION.

THE COURT: FINE. OKAY.

ALL RIGHT. WE WILL COME BACK TO THE SPECIFIC

AREAS, IF I DO WISH TO HEAR FROM HIM, SPECIFIC AREAS THAT I'M INTERESTED IN. I'LL ACCEPT IT NOT AS GOSPEL TRUTH OF WHAT IT IS; I MAKE THAT DECISION; BUT I'D LIKE TO KNOW WHAT THE ATTITUDE IS AND THE INTERPRETATION MIGHT BE OF OTHER PEOPLE. AND I CAN BE SPECIFIC AS I WANT HERE.

AND IF THERE IS INCONSISTENCY WITH WHAT HE SAID IN A DEPOSITION, THEN YOU CAN BRING IT UP. OKAY?

MR. SCHLAFLY: OKAY.

THE COURT: OKAY. 1:30.

(LUNCH RECESS TAKEN AT 11:57 A.M.)

(PROCEEDINGS RESUMED AT 1:37 P.M.)

THE COURT: I DON'T BELIEVE I NEED ANY MORE TESTIMONY AT THIS TIME. SO WE WILL DISPENSE WITH FURTHER TESTIMONY. IF I NEED ANY MORE EXTRINSIC EVIDENCE, I MAY CALL YOU. BUT I THINK THAT WE'RE SATISFIED NOW.

I WOULD LIKE TO ARGUE IT, THOUGH, ON THE APPLICATION OF SECTION 112, PARAGRAPH SIX, TO THE CLAIMS IN THIS CASE. NOTHING CRITICAL TO UNDERSTAND THAT. SO I WELCOME ARGUMENT ON THAT.

AFTER WE CONCLUDE THAT, I WILL HEAR THE MOTION FOR REMAND.

MR. HASLAM?

MR. HASLAM: THE COURT HAS ASKED US TO ADDRESS THAT, AND I THINK THAT THERE WAS ONE POINT THAT THE BRIEFS MADE CLEAR, THE VOLUMINOUS BRIEFS MADE CLEAR, WAS THAT THE

APPLICATION OF 35, 112, PARAGRAPH SIX TO THIS CASE, IS ONE OF THE PRINCIPAL ISSUES THAT WE'RE HERE TO DECIDE.

THE COURT: RIGHT.

MR. HASLAM: AND THE SIGNIFICANCE OF THAT IS PLAINLY THIS: IF THE CLAIMS, IN PARTICULAR, CLAIMS 1 TO 5, ARE SUBJECT TO THAT -- BECAUSE THERE IS NO DISPUTE THAT CLAIM 6 IS SUBJECT TO 35, 112, PARAGRAPH SIX -- THEN THE INVENTION IS LIMITED TO THE DISCLOSED EMBODIMENTS, OR THEIR EQUIVALENTS. AND HERE, THAT WOULD BE THE TRAP DOOR KNAPSACK, OR ITS EQUIVALENTS, IF THERE ARE ANY.

WHAT WE REALLY ARE DISCUSSING HERE ARE REALLY MATTERS OF SUBSTANCE, AND I THINK TO SOME EXTENT, LOST IN THE RHETORIC, AND PERHAPS DESIGNEDLY SO, BY CYLINK, TO TREAT IT REALLY AS A SEMANTIC ISSUE AND ONE OF WHETHER MAGIC WORDS APPEAR OR NOT. AND I WILL GET LATER TO WHAT I THINK THE COURTS HAVE SAID ABOUT THE SIGNIFICANCE OF THAT.

BUT I THINK WHAT WE'RE REALLY DEALING WITH HERE IS: IT IS AN UNDERLYING PRINCIPLE OF THE PATENT LAW THAT GOES BACK TO THE MORSE CASE, AND IS STILL GOOD LAW TODAY, AND IT'S A MORE FUNDAMENTAL CONCERN. AND IT'S NOT THE SEMANTIC CONCERN OF: CAN I GO TO A DICTIONARY AND FIND THE DEFINITION OF A PARTICULAR WORD.

IT IS: ARE THE CLAIMS, WHEN SO CONSTRUED, ARE THE CLAIMS, WHEN YOU'VE GONE TO THE DICTIONARY, OF SUCH INDEFINITENESS OR BREADTH, DO THEY TALK MORE ABOUT THE

DESIRED RESULT THAN REALLY HOW TO DO IT, DO THEY SWEEP TOO BROADLY. THAT'S WHAT WE'RE REALLY TALKING ABOUT HERE.

AND I WILL BE THE FIRST TO ADMIT THE LINE IS NOT A BRIGHT LINE, AS IT FREQUENTLY ISN'T. IN MANY AREAS OF THE LAW, AND I WOULD VENTURE TO SAY IN THE PATENT AREA, THERE ARE MANY DICTUMS THAT THE COURTS LAY DOWN. WHEN YOU, AT THE TRIAL LEVEL, HAVE TO APPLY THEM, THEY AREN'T AS EASY AS THEY SEEM AT THE APPELLATE LEVEL.

BUT I DO BELIEVE HERE THAT WE'VE PRESENTED A CONVINCING CASE, AND I WILL ARGUE IT, THAT ON THIS ONE, WE CLEARLY ARE ON THE OTHER SIDE OF THE LINE.

THESE CLAIMS, IF THEY MEAN NOTHING MORE THAN WHAT CYLINK SAYS, REALLY DO SEEK TO PATENT THE FUTURE. THEY REALLY ARE INIMICAL TO THE PURPOSES OF THE PATENT STATUTE, WHICH ARE TO FOSTER INNOVATION RATHER THAN TO STIFLE IT.

NOW, THE CASE LAW -- AND WE'LL TURN TO THE CASE LAW -- IS NOT NEARLY AS VOLUMINOUS AS CYLINK WOULD HAVE YOU BELIEVE. NOW, THEY DID A VERY IMPRESSIVE JOB OF BRIEFING AND REBRIEFING AND SUPPLEMENTALLY BRIEFING THE ISSUE OF 112.6, AND THEY HAVE GIVEN THE COURT MANY APPENDICES OF CASES.

AND WE WILL, TO THE EXTENT NECESSARY, WE HAVE GONE THROUGH THEM, AND WE CAN PROVIDE A SUMMARY RECITATION OF WHAT THOSE CASES REALLY STAND FOR. AND WE CAN DO THAT,